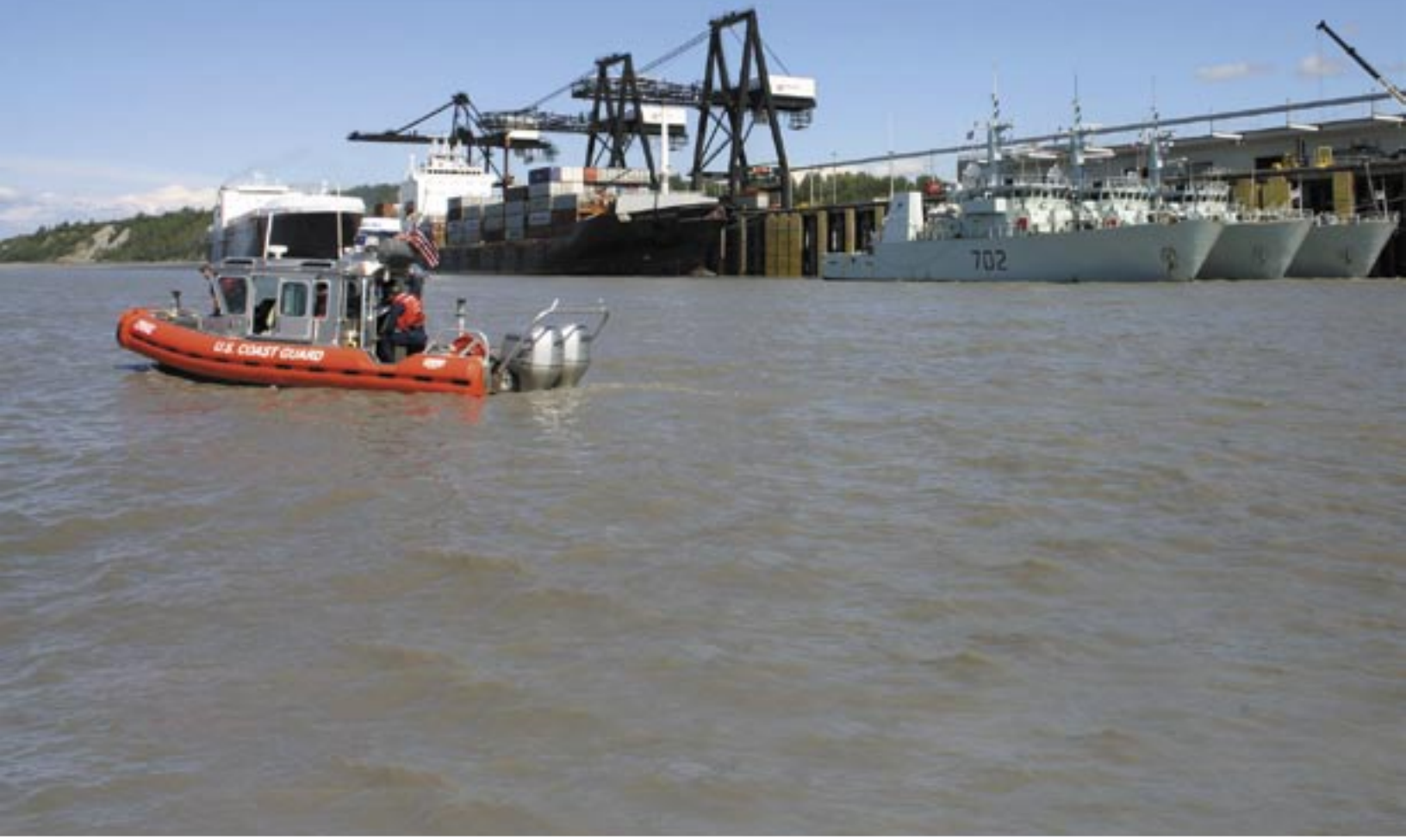
PORT AND SUPPLY-CHAIN SECURITY INITIATIVES IN THE UNITED STATES AND ABROAD



Lyndon B. Johnson School of Public Affairs
The University of Texas at Austin
Policy Research Project Report

150

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Port and Supply-Chain Security Initiatives in the United States and Abroad	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **University of Texas at Austin,Lyndon B. Johnson School of Public Affairs,Austin,TX**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**238**	

Lyndon B. Johnson School of Public Affairs
Policy Research Project Report
Number 150

Port and Supply-Chain Security Initiatives in the United States and Abroad

Prepared for the

Congressional Research Service

Project Directed by

Leigh B. Boske

A report by the Lyndon B. Johnson School of Public Affairs
Policy Research Project on Port and Supply-Chain Security
2006

The LBJ School of Public Affairs publishes a wide range of public policy issue titles. For order information and book availability call 512-471-4218 or write to: Office of Communications, Lyndon B. Johnson School of Public Affairs, The University of Texas at Austin, Box Y, Austin, TX 78713-8925.
Information is also available online at www.utexas.edu/lbj/pubs/

ISBN-10:0-89940-763-3
ISBN-13: 978-0-89940-763-0

©2006 by The University of Texas at Austin.
All rights reserved. No part of this publication or any corresponding electronic text and/or images may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher.

Printed in the U.S.A.

Cover by Doug Marshall
LBJ School Communications Office

Policy Research Project Participants

Project Director

Leigh B. Boske, Ph.D.
Associate Dean and Professor, Lyndon B. Johnson School of Public Affairs

Students

Claudia M. Arniella, B.S. (International Affairs and Spanish), Georgia Institute of Technology

Nissa Brown, B.A. (European Cultural Studies), Brandeis University

Jacqueline S. Carton, B.A. (French), University of Texas at Austin

Eric R. Christensen, B.S. (Foreign Service), Georgetown University

John C. Cuttino, B.A. (History), Tufts University; M.P.Aff (Public Affairs), University of Texas at Austin

Lindsey Ford, B.M. (Vocal Performance), Samford University

Kathryn A. Koch, B.A. (International Studies and French), Baylor University

Renée E. Leta, B.A. (Communications), University of Pennsylvania

Lt. Troy Roberts USN, B.B.A. (International Business), Grand Canyon University

Amy N. Shuart, B.A. (Public and Urban Affairs and Political Science), Virginia Polytechnic Institute and State University

Leya B. Speasmaker, B.A. (English), University of Virginia; M.T. (Teaching), University of Virginia

Ben Stark, B.A. (Economics and Psychology), University of Texas at Austin

Shauntel Taylor, B.A. (English), University of Texas at Austin

David L. Trachtenberg, B.A. (Sociology), Brandeis University

Matt Williams, B.A. (Political Science and Economics), Rice University

Forward

The Lyndon B. Johnson School of Public Affairs has established interdisciplinary research on policy issues as the core of its educational program. A major part of this program is the nine-month policy research project, in the course of which one or more faculty members from different disciplines direct the research of ten to thirty graduate students of diverse backgrounds on a policy issue of concern to a government or nonprofit agency. This "client orientation" brings the students face to face with administrators, legislators, and other officials active in the policy process and demonstrates that research in a policy environment demands special talents. It also illuminates the occasional difficulties of relating research findings to the world of political realities.

This report is the product of a Policy Research Project conducted during the 2005-06 academic year with funding from the Congressional Research Service of the U.S. Congress. The purpose of the study is to provide a comprehensive overview of U.S. and foreign strategies to enhance port and supply-chain security.

The curriculum of the LBJ School is intended not only to develop effective public servants but also to produce research that will enlighten and inform those already engaged in the policy process. The project that resulted in this report has helped to accomplish the first task; it is our hope that the report itself will contribute to the second.

Finally, it should be noted that neither the LBJ School nor The University of Texas at Austin necessarily endorses the views or findings of this report.

James Steinberg
Dean

Acknowledgments

This policy research project was made possible by contributions from a significant number of people. We are especially grateful to Jennifer Lake, Analyst in Domestic Security at the Congressional Research Service, and to Jacqueline Carton and Lindsey Ford, the copy-editors of this report. We also thank the following individuals for participating in the project and sharing their invaluable insights:

Miriam Lopez Alman, Director of the Department of Maritime Traffic, Mexican Customs, Veracruz, Mexico

Wade Battles, Managing Director, Port of Houston Authority, Houston, Texas, USA

Katia Bennett, Desk Officer for Hong Kong, Office of Chinese and Mongolian Affairs, Bureau of East Asian and Pacific Affairs, U.S. Department of State, Washington, D.C., USA

Stefan Bjorkencrona**,** National Expert, Taxation and Customs Union Directorate-General, European Commission, Brussels, Belgium

Justice Blose, Port Security Officer, National Ports Authority, Durban, South Africa

Paul Booysen, Port Security Officer, National Ports Authority, Cape Town, South Africa

Captain Eddie Bremner, Harbor Master, Cape Town, South Africa

François Brivet**,** Co-Director, Regional Customs Office of Marseille, Marseille, France

Nathalie Bureau du Colombier, Journalist, *L'Antenne*, Marseille, France

Bruno Carpentier, Chief Executive Officer, MGM, Marseille, France

Ernani Checcucci, Technical Officer Customs Modernization, Capacity Building Directorate, World Customs Organization, Brussels, Belgium

Sunny Chen, General Manager, COSCO-HIT Terminals, Hong Kong SAR, China

Ricky Chiu, President, Grand Power Logistics Group LTD, Hong Kong SAR, China

George Chu, Hutchison Port Holdings, Hong Kong SAR, China

Captain Raymundo Mata Contreras, Deputy Director General, Secretary of Communications and Transportation, Mexico City, Mexico

Vice Admiral Vivien Crea, Commander Atlantic Area, United States Coast Guard, Portsmouth, Virginia, USA

Charles Diorio, Director, Government Affairs, World Shipping Council, Washington, D.C., USA

Sander Doves**,** Policy Advisor for Strategy, Infrastructure, and Maritime Affairs, Port of Rotterdam, Rotterdam, the Netherlands

Theo W. Fletcher**,** Vice President, Import Compliance and Supply-Chain Security, IBM Corporation, Somers, New York, USA

Peter J. Gatti**,** Jr., Executive Vice President, National Industrial Transportation League, Reston, Virginia, USA

Captain Manuel F. Gutiérrez Gallardo, Assistant Director of Port Protection, APIVER, Port of Veracruz, Veracruz, Mexico

Lieutenant Kelley Hall**,** Aide to Commander Atlantic Area, United Sates Coast Guard, Portsmouth, Virginia, USA

Lucas Haluodi, Chief Executive Officer, South African Maritime Safety Authority, Pretoria, South Africa

Paul Ho, Port Facility Security Officer, Hutchison International Terminals, Hong Kong SAR, China

Jozef Hupperetz**,** Supply Chain Security, Taxation and Customs Union Directorate-General, European Commission, Brussels, Belgium

Robert Ireland, Technical Attaché, Capacity Building Directorate, World Customs Organization, Brussels, Belgium

Hans Ittmann**,** Manager, Logistics and Quantitative Methods, Built Environment, Council for Scientific and Industrial Research, Pretoria, South Africa

Guy Janin, Port Director, Port of Marseille, Marseille, France

Jan Kamp**,** Project Manager, Customs Rotterdam, Rotterdam, Netherlands

Abhay Kantak**,** Manager, Infrastructure Advisory, Urban, CRISIL Limited, Mumbai, India

Joe Kelly, Columbus Programme Manager, Capacity Building Directorate, World Customs Organization, Brussels, Belgium

Chris Kennedy, LBJ School of Public Affairs, University of Texas at Austin, Austin, Texas, USA

Castro Khwela**,** Intelligence and Investigations Manager, National Ports Authority, Durban, South Africa

Chris Koch, President and CEO, World Shipping Council, Washington, D.C., USA

John Kok, General Manager-CSI, Hutchison Port Holdings, Hong Kong SAR, China

Derik Latham, Assistant to the Director, International Association of Airport and Seaport Police, Vancouver, Canada

Henry Lee, Executive Director, Hong Kong Container Terminal Operators Association Limited, Hong Kong SAR, China

Captain Rufus Lekala, Deputy Harbor Master, Port of Cape Town, Cape Town, South Africa

Vicente Angel Linares, Protection Official and Assistant Director of Operations, ICAVE, Veracruz, Mexico

Miguel Mario Inzunza Luque, Assistant Administrator of Customs Operations, Mexican Customs, Veracruz, Mexico

Jean-François Mahé, Vice President of Container Logistics, CMA-CGM, Marseille, France

Jean-Pierre Marcorelles**,** President, Freight-Forwarding Association for Multimodal Transport, Marseille, France

Juan Martinez**,** Terminal Manager, MGM, Marseille, France

Emma Maspero**,** Logistics Analyst, Council for Scientific and Industrial Research, Stellenbosch, South Africa

Andrew Maswanganye, Director of Maritime Safety, Security and Bilateral Affairs, Department of Transportation, Pretoria, South Africa

Ruben Medina, Operations Manager, APIVER, Veracruz, Mexico

Romeo Minnie, South Africa Revenue Service – Customs, Durban, South Africa

Captain Jitendra Mishra, Deputy Conservator of Port, Jawaharlal Nehru Port Trust, Mumbai, India

Saleem Modak, South African Maritime Safety Authority, Pretoria, South Africa

Billy Mokale, South African Maritime Safety Authority, Pretoria, South Africa

Mark Motley, Political Director, Embassy of the United States in France, Paris, France

Joseph Moysan, Harbor Master, Port of Marseille, Marseille, France

Gerrie Mulder, National Intelligence Agency, Pretoria, South Africa

Captain Girish J. Munjal, Manager, QHSE & Training, Nava Sheva International Container Terminal Pvt. Ltd., Mumbai, India

Qiniso Mzobe, National Intelligence Agency, Pretoria, South Africa

Gugu Ndebele, Department of Tranportation, Pretoria, South Africa

Captain Karl Otto, Deputy Harbor Master, Cape Town, South Africa

Gabriela Martinez Ramirez, Supervisor of Customs Operations, Mexican Customs, Veracruz, Mexico

Kerwin Rampono, Head of National Maritime Security Operations, National Port Authority, Pretoria, South Africa

Richard Reiter, Senior Desk Officer for the Netherlands and Luxembourg, U.S. Department of State, Washington, D.C., USA

Marc Reverchon, President, Union of Maritime Professionals at Marseille-Fos, Marseille, France

Serge Rinkel, European President, International Association of Airport and Seaport Police, Rezé, France

Beth Ann Rooney, Director of Port Security, Port Authority of New York and New Jersey, New York, New York, USA

Tanya Saade, Vice President of Corporate Communication, CMA-CGM, Marseille, France

Peter Schmidt, Analyst/GIS, Council for Scientific and Industrial Research, Pretoria, South Africa

Selma Schwartz, Marketing Manager, National Ports Authority, Cape Town, South Africa

Captain Sujeet Singh, General Manager of Operations, Nava Sheva International Container Terminal Pvt. Ltd., Mumbai, India

Ambassador Craig Roberts Stapleton**,** American Ambassador to France, Embassy of the United States in France, Paris, France

Hennie Strydom, Port Facilities Security Officer, National Ports Authority, Durban, South Africa

Henry Sze, General Sales Manager, Grand Power Logistics Ltd., Hong Kong SAR, China

Christian Taormina**,** Organization and Information Systems Director, MGM, Marseille, France

Vusumzi Tito, South African Police Services, Pretoria, South Africa

Mike Toddington, Executive Director, International Association of Airport and Seaport Police, Vancouver, Canada

Jason Tsang, Port Facility Security Officer, Modern Terminals Ltd., Hong Kong SAR, China

Decky Tse, General Manager, Grand Power Logistics Ltd., Hong Kong SAR, China

S.A. Usmani, Joint Commissioner, Jawaharlal Nehru Customs House, Ministry of Finance, Government of India, Mumbai, India

Bruno Vaccà**,** Administrator in Chief of Maritime Affairs and Maritime Defense, Ministry for Transport, Infrastructure, Tourism and the Sea, Paris, France

Myra van der Merwe, National Intelligence Agency, Pretoria, South Africa

Henk van Unnik, Director of Foreign Projects, Integrated Risk-Management Associates, Rotterdam, Netherlands

Russell Whitmarsh, Director of Port Security, Port of Houston Authority, Houston, Texas, USA

Christopher J. Wilson, Superintendent of Police, DVC KTDIV, Hong Kong SAR, China

Alexander Wong, Senior Logistics Officer, Grand Power Logistics Ltd., Hong Kong SAR, China

W.H. Wong, Senior Marine Officer, Hong Kong Marine Department, Hong Kong SAR, China

R.K.B. Yadav, Deputy Manager Operations, Jawaharlal Nehru Port Trust, Mumbai, India

Executive Summary

Between 1990 and 2004, the value of U.S. international trade increased from $889 billion* to nearly $2.2 trillion. Roughly two-thirds of this total value of trade passed through U.S. freight gateways (primarily ports) to and from countries other than Canada and Mexico. The top 50 U.S. ports accounted for about 90 percent of all maritime cargo tonnage; and 25 U.S. ports accounted for 98 percent of all container shipments. In 2004 alone, the liner shipping industry transported $1.5 billion worth of containerized goods, through U.S. ports, every day. All told, roughly 10 million loaded cargo containers entered the U.S. in 2004.

Given universal recognition that cargo containers may be used to smuggle chemical, biological, radiological, or nuclear weapons, it is understandable that "*assuring container security*" has become a priority to governments and the international trade community alike to prevent incidents of mass destruction and major disruptions to the world economy. Mike Toddington, Executive Director of the International Association of Airport and Seaport Police, has noted that public officials must walk a fine line in devising methods that simultaneously secure ports and facilitate trade. Promoting both security and trade facilitation requires the examination of global supply chains. Cargo container movements, between points of origin and their ultimate destinations, are characterized by complex interactions among multiple actors, industries, regulatory agencies, modes of transportation, operating systems and legal frameworks.

On behalf of the Congressional Research Service, the Lyndon B. Johnson School of Public Affairs at the University of Texas at Austin, conducted research during the 2005-06 academic year to examine the various institutional, legal and policy arrangements that have been put into place in the U.S. and abroad to enhance worldwide port and supply-chain security. Researchers collected information from literature reviews, websites, telephone interviews, and site visits to a number of U.S. and foreign ports and agencies. Interviews were conducted with officials in government agencies, international organizations, ports, and private-sector firms and associations. This executive summary highlights key findings and lessons learned.

Contents

This report is composed of eleven chapters. Chapter 1 presents a primer that details the roles and interactions of key government agencies and international organizations, the security initiatives for which they are responsible, and the various ways in which the private sector contributes to and participates in security processes.

Chapter 2 discusses the International Maritime Organization's (IMO) International Ship and Port Facility Security Code (ISPS), which provides a common international framework with which to assess security vulnerabilities and threats, implement security measures, respond to security incidents, and facilitate international cooperation. ISPS is

* Unless otherwise noted, all currency is listed in U.S. dollars.

based on the U.S.' Maritime Transportation Security Act (MTSA) of 2002, an amendment to the U.S. Merchant Marine Act, designed to protect U.S. ports and waterways from terrorist attacks.

Chapter 3 addresses the Customs-Trade Partnership Against Terrorism (C-TPAT), a joint-U.S. government/business initiative to build cooperative relationships designed to secure global supply chains. C-TPAT, a voluntary program, has become a key component of the U.S. Customs and Border Protection's (CBP) security enhancements in the post 9-11 environment and, therefore, is of significant importance to this report. The findings of a C-TPAT survey, administered electronically to members of the National Transportation Industrial League (NITL), are also presented. In addition, the chapter describes supply-chain security initiatives developed by the European Union and IBM Corporation.

Chapter 4 highlights the World Customs Organization's (WCO) SAFE Framework of Standards to Secure and Facilitate Global Trade (known as SAFE). SAFE compiles best practices for Customs administration security and trade facilitation, and establishes an agenda for business participation, authorization, and inter-country Customs communication. Also discussed is the role of the WCO within the international community, as well as its relationship with CBP.

Chapters 5 through 11 contain seven case studies: Brazil and the Port of Santos; France and the Port of Marseille; Hong Kong and the Port of Hong Kong; India and the Port of Jawaharlal Nehru; Mexico and the Port of Veracruz; the Netherlands and the Port and Rotterdam; and South Africa and the Ports of Cape Town and Durban. Each case study consists of two parts. The first part examines national port security, Customs regimes, and national port administration. The second part provides an overview of security structures and processes implemented at specific ports, including the ISPS and the Container Security Initiative (CSI).

Key Findings and Lessons Learned

International Ship and Port Facility Security Code (ISPS)

The International Ship and Port Facility Security Code (ISPS) was adopted in 2002 as a measure to enhance maritime security under the IMO's International Convention for the Safety of Life at Sea (SOLAS). Acting as the international counterpart to the U.S.' Maritime Transportation Security Act (MTSA), ISPS establishes a baseline requirement for the 159 contracting governments to the SOLAS convention and provides a common international framework with which to assess security vulnerabilities and threats, implement security measures, respond to security incidents, and facilitate international cooperation.

ISPS, which specifies standards for contracting governments, government agencies, local administrations, ports and the shipping industry,[1] is divided into two parts. Part A consists of mandatory regulations delineating the basic responsibilities for governments, port authorities, and shipping companies, while Part B provides voluntary guidelines on how to meet those requirements.[2]

Our research revealed an abundance of conflicting views on both ISPS and its domestic counterpart, MTSA. Several trade journal articles, for example, posited that the MTSA does not address viable security risks and proffered that terrorists would, in a real-life scenario, do everything in their power to comply with MTSA guidelines so as not to draw attention to themselves and/or their vessel.[3] Additionally, many port security officers feel that the implementation of MTSA has increased their workloads by "unreasonable" amounts.

Our research on ISPS at international ports revealed similar disenchantment, though more as a result of implementation policies and financing, than with personnel problems. Most of the criticism stems from a near consensus among international players that ISPS mainly supports U.S. interests. Countries, critics argue, are virtually forced to participate out of a fear of being abandoned by trade partners.

Funding for both the MTSA and ISPS is another source of contention for most players, as implementation, equipment, and maintenance required by both initiatives has fallen mainly to the ports and, in many cases, the private-sector terminal operators at the ports. In the U.S., for example, though MTSA legislation calls for Congress to cover roughly 75% of implementation costs, Congress has not met this mandate and ports have been responsible for securing their own funding. Smaller ports, in particular, are struggling to implement MTSA with little financial aid, as 'at-risk' ports currently receive the majority of available funding. [4]

The question of funding for ISPS implementation and maintenance also remains up for debate. ISPS mandates affect many different agencies, shippers, ports and contracting governments and no two entities are funding it in exactly the same way. This financial crisis is further exacerbated by the feeling of many contracting governments that the benefits realized from compliance do not outweigh the costs involved.

The most poignant lessons learned in our evaluation of ISPS came from country-specific research and site visits. During these visits it became clear just how inconsistent ISPS is from port to port and country to country. While the language of ISPS is uniform in each port and each country, it was as if we were seeing seven different codes. Not only has ISPS been implemented in different ways and with varying levels of success, but overall opinions of ISPS among shippers, port workers and government officials fluctuate as well. For a more in depth overview of these lessons learned, please refer to the last section of the Executive Summary entitled Country and Port Case Studies.

The inconsistencies in implementation methods from country to country, as well as differing opinions on ISPS, serve to reiterate the importance of harmonization and international standards. Our research highlights many of the financial and ideological discrepancies in different countries that must be taken into consideration when developing and trying to implement such globally significant legislation.

Much important work remains to be done on the MTSA and ISPS initiatives if their requirements are to be successfully and cohesively implemented. Unfortunately, this need is overshadowed by the multitude of new port security initiatives and legislation

continually being created. Both individual countries and the international community must renew their focus on existing programs and legislation.

Customs-Trade Partnership Against Terrorism (C-TPAT)

The Customs-Trade Partnership Against Terrorism (C-TPAT) was established in 2001 in an effort to address the threat of a terrorist attack on the global supply chain. C-TPAT is a voluntary, government/private-sector partnership that works to enhance the security of the entire supply chain, as well as to build cooperative relationships between the public and private sectors.[5] In exchange for tightened security and cargo tracking at points along the supply lines, C-TPAT offers participants expedited cargo processing, Customs reviews, recommendations and best-practice information.

Our decision to look closely at this particular security initiative was a result of its widely varying and highly contentious reviews. For example, while most government reports and websites present C-TPAT as the U.S.' foremost and most comprehensive "anti-terror initiative,"[6] industry respondents believe that it is not operating efficiently. In fact, most private-sector representatives feel that C-TPAT is an inadequately funded and managed program that requires costly, if not cost-prohibitive, security measures.

The following are the most prevalent criticisms of C-TPAT:

- CBP has not concretely defined member benefits;
- There is inconsistency in the steps of the certification process at which participating firms are granted benefits;
- The validation process for firms is not comprehensive; and
- CBP does not have the personnel necessary to complete the validations in a timely manner.[7]

Perhaps most important is the critique, offered by prominent trade journals, that many of the changes to and decisions about C-TPAT have been made without adequate private-sector consultation.[8] Further, public and private players alike, seem to feel that CBP is sending a mixed message by naming security as its number one priority, while implementing C-TPAT as a voluntary program.[9]

In analyzing the varied responses to C-TPAT, we found that the shipping industry was not well-represented in the debate. To that end, our researchers designed a comprehensive survey, distributed electronically in February 2006 by the National Industrial Transportation League (NITL) to its member companies, to identify the shipping industry's responses to and opinions about C-TPAT. Questions were developed that allowed the shipping industry an opportunity to comment, confidentially, on various aspects of C-TPAT. The survey was also designed to gain a sense of the types of firms participating in C-TPAT and the reasoning behind their decisions to do so.

Of the forty-four firms that responded to the survey, nearly 80 percent of respondents were C-TPAT members. One of the most valuable aspects of the survey was the section in which firms provided anecdotal comments about their experiences with and opinions of C-TPAT. The comments centered on such themes as the lack of resources provided to fund the program; the need for increased knowledge and skill for C-TPAT enforcers and valuators; and the need for program flexibility in order to accommodate different types of firms.

Overall sentiments about C-TPAT, as reflected in both respondents' answers to questions and their supplementary comments, are as follows:

1. The idea behind C-TPAT is good and, with work, it could achieve the balance of facilitating trade growth while simultaneously strengthening supply-chain security. However, Congress is ill-equipped to effectively monitor or regulate any import-related processes as it lacks the necessary understanding of the international supply chain.

2. CBP is slow, highly bureaucratic and officials are often poorly trained, particularly in validation of C-TPAT participants. The bureaucracy makes for a confusing and habitually inefficient process.

3. C-TPAT is a good first step but, in order to reach its potential, must either be made a mandatory initiative or firms must actually realize the benefits advertised.

4. As with many U.S. initiatives that are wholly applicable to the international community, C-TPAT must be extended to foreign governments and international industry participants as it is virtually useless without foreign participation.

Overall, firms at all levels of the supply chain acknowledge and support the need for an industry-wide security initiative. To date, however, industry pressures to join C-TPAT do not outweigh the perceived lack of advantages to participating in the program or the costs a firm must bear in order to be validated. Much work remains to be done to include the opinions and suggestions of private-sector participants in future planning stages of C-TPAT, as well as to create avenues through which the international trade community can participate.

The World Customs Organization and the SAFE Framework of Standards to Secure and Facilitate Global Trade

The SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE) is a voluntary, international initiative of the World Customs Organization (WCO) adopted in June 2005. SAFE was developed in an effort to modernize Customs regimes while creating standardized international practices and increased efficiency through training in new technologies and human resource management, coupled with an emphasis on systemic integrity building.

While the current push from the United States is to strengthen security and specifically to deter possible terrorist attacks, the WCO has recognized that the goals for Customs

modernization in other countries are more diverse, focused instead on trafficking of counterfeit goods, intellectual property rights, and collection of duties. With this in mind, the WCO conceived of SAFE, a framework designed to challenge each member country to use its national goals in order to develop a unique Customs administration.

In comparison to previous initiatives, the WCO has received an unprecedented number of member-country pledges to implement SAFE.[10] Member-country support for SAFE ranges from monetary contributions to in-kind support, such as site assessments and training. While commitment to SAFE is voluntary, the general belief is that countries will be at a competitive disadvantage for international trade if they do not participate.

SAFE consists of two major 'pillars' and a capacity-building component. The Customs-to-Customs Pillar, which is described as resembling parts of the U.S.' Container Security Initiative (CSI) and other CBP-led anti-terror initiatives, aims to provide harmonized Customs standards in an attempt to encourage and facilitate international cooperation and information sharing. Concerns, however, have already been raised about the pillar which advocates that Customs administrations focus on exports. For the many developing countries that still rely on import revenues for government funding,[11] independent reviewers anticipate difficulties in shifting towards more export-focused or 'outbound' Customs administrations.

Much like the U.S.' C-TPAT program,[12] SAFE's Customs-to-Business Pillar is rooted in the idea that, in order to maximize efficiency and effectiveness in securing the international trade supply chain, Customs administrations must partner and collaborate with the private sector. This pillar has been enhanced by the WCO's creation of a Private Sector Consultative Group (PSCG) which provides the WCO with industry recommendations on security and trade facilitation.

Finally, the Columbus Programme is SAFE's capacity-building initiative. Its goal is to promote the adoption and implementation of SAFE while building sustainable, long-term capabilities for Customs administrations.[13]

The greatest challenge facing SAFE will be for member countries to legislate more authority for their Customs administrations to oversee export-related activities.[14] SAFE is a long-term commitment to Customs modernization and strategic planning. In spite of pledged funding, diagnostic missions and private-sector support, systemic change in many Customs administrations may come slowly due to a lack of political will within member countries. Further, each participating country will enter the implementation stage at a different level of interest and capability. As such, it will take a long time before member countries and private-sector participants are on a 'level playing field.'

Country and Port Case Studies

Although the countries selected for this report are extremely diverse, politically, economically and geographically, several common themes emerged during the on-site port interviews. One of the most striking findings that is mentioned in each port study is the fundamental incongruity between the maritime security priorities of the U.S. and

those of other countries. Port officials expressed universal recognition of the importance of a secure global supply chain. However, in no port interview did an official cite terrorist activities as a primary security concern. Instead, smuggling, fraud and human trafficking were universally cited as security priorities of far greater consequence. In those ports that did acknowledge concerns about terrorism, such as Hong Kong, this concern was motivated far more by the economic consequences of a terrorist event than by fear of a domestic attack.

In the same way that U.S. security initiatives have been prompted and shaped by the events of 9/11, the security structures of other nations reflect their respective domestic experiences and political concerns. One of the greatest impediments to supply-chain security is the lack of uniformity across international security structures and initiatives. While the U.S. has recently overhauled its maritime regime, the administrative and organizational structures of foreign ports typically pre-date 9/11. Although ports have been working to implement the operational changes mandated by ISPS and CSI, most of their existing maritime structures remain. The U.S. federal government must recognize that the pace of structural change tolerated by foreign interests is likely to be slower than it might hope.

In spite of differing security priorities, many officials expressed appreciation for some of the positive changes that have resulted from ISPS and CSI. The majority of port officials interviewed perceive the greatest benefit of ISPS and CSI to be the increased overall awareness of security issues and procedures these programs have brought to their ports. Port administrators in Mexico, South Africa and India also noted the achievement of significant efficiency gains as a result of the programs' implementation. Although these new initiatives are bringing about positive changes, they represent a paradigmatic shift in security protocols for many countries, and will still require some time to be completely integrated.

One of the areas in which a lack of international uniformity is most evident is the role played by Customs agencies in port security. The primary focus of Customs agencies has typically been revenue collection and trade facilitation, while security responsibilities – generally performed by other agencies - have revolved around the prevention of fraud and smuggling. The U.S. emphasis on pushing its borders outward represents a fundamental change in the focus and practices of Customs agencies. The dual mandate of revenue collection and security promotion has left Customs agencies with goals that often appear to be in direct conflict with each other. Officials acknowledged the difficulty in finding an adequate balance between these two goals. For many countries, especially those in weaker financial situations, revenue generation remains a greater priority. Indian officials cited concerns that CSI would hinder outgoing trade as the primary impediment to CSI implementation. Similarly, South African officials cited economic concerns as the primary reason that non-ISPS compliant vessels are often allowed to enter their ports. In order to overcome these difficulties, the U.S. should increase its work with the WCO to provide an open forum for international dialogue on the role of Customs agencies. International standards must better account for the differing needs of all involved parties if they are to be fully accepted and integrated.

One of the most prominent sentiments expressed by interviewees is the need for better inter-governmental communication and coordination. Although U.S. policy has advocated overlapping security initiatives as a means of ensuring comprehensive maritime security, the sudden abundance of new security mandates has become overwhelming and confusing for many countries. Multiple initiatives also create redundancies that could be avoided if nations and agencies communicated more clearly about their plans. France, South Africa and India all cited better intelligence-sharing and communication as top priorities for global maritime security. Other countries complained that international security initiatives are often given as mandates, without proper explanation or adequate guidelines. South Africa identified a lack of adequate guidelines as its greatest obstacle to ISPS implementation. In order to remedy these problems, French officials requested that the U.S. ensure the fluid and complete implementation of its current programs before introducing new initiatives.

In speaking with foreign officials, it became evident that widespread displeasure over the U.S.' pursuit of a unilateralist foreign policy extends to maritime security issues. Although the U.S. was the driving force behind both ISPS and CSI, ISPS has been more broadly and easily accepted by other nations. The multilateral nature of ISPS creates the perception that the program is more concerned with worldwide maritime security than solely with U.S. national interests. Additionally, the IMO's administration of ISPS seems to be viewed as a more inclusive and benign form of leadership than the U.S.' oversight of CSI.

Broader acceptance of ISPS was made evident, both explicitly and implicitly, during our port interviews. All of the countries studied have signed on to the ISPS and CSI programs; however, two countries, Mexico and India, have yet to implement the CSI program. Although officials in both nations expressed a continued commitment to the program, no formal plans or timelines have been drafted. In contrast, ISPS implementation is underway in all of the countries interviewed, and has been completed in every country except for Brazil. Some officials complained that U.S. programs such as CSI are experienced internationally as being forced upon other nations, with the expectation that the lure of U.S. trade will provide sufficient leverage for the program's acceptance. Such an approach on the part of the U.S. may bring short-term rewards, but carries with it significant long-term repercussions. In the long-term, those countries that can afford to do so might be tempted to emphasize trade with other nations and minimize their need to implement the stringent requirements mandated by the U.S. Those countries that rely heavily on U.S. trade may continue to comply, but this leveraged compliance will only engender further resentment and animosity towards U.S. unilateralism.

Another theme discovered during port interviews is the concern that the costs of implementing maritime security initiatives are often prohibitively high and unevenly distributed. The financial burden of security initiatives has fallen most heavily on developing countries and the private sector. South Africa, Brazil and India, all of which rely primarily upon their federal governments for port funding, experienced the greatest difficulties in financing security initiatives.

Many national governments have been able to minimize financial burdens by decentralizing port administrations and operations. This strategy has been mimicked at all levels of government, creating a successive devolution of financial responsibility. As a result, private terminal operators and port authorities often shoulder the primary financial burden for financing new security initiatives. Brazilian terminal operators reported passing these costs along to port users through higher rates, while Mexican port officials plan to introduce a per-container tariff to cover the costs of CSI implementation. These strategies are not unique to poorer nations. In France, one of the more prosperous nations included in this report, the state has not provided any funding for ISPS implementation, although its autonomous ports all remain under the national government's financial control. As a result, French operators have also instituted higher user rates at their terminals.

Increased private-sector financing and participation in port security create both opportunities and obstacles to supply-chain security. Large port operators are frequently able to harness resources more easily than fiscally constrained government agencies. In India and France, private operators have instituted far more rigorous security measures than their public counterparts, and Hong Kong terminal operators jointly financed an innovative pilot project to provide for 100% screening of container shipments. Private companies have also been quicker to acknowledge the importance of comprehensive supply-chain security. Programs such as the Smart and Secure Trade Lanes Initiative take an inclusive view of maritime security, engaging both governments and private companies in order to secure the entire supply chain.

However, private port financing of security initiatives introduces another set obstacles to achieving port security. The financial costs of security initiatives are often prohibitively high for smaller terminal operators. South Africa reported significant difficulties with low-pay, private security officers who are frequently less reliable and lax in their duties, and the Netherlands recounted difficulties in enforcing ISPS implementation with smaller operators. Even large private terminal operators, such as Hutchison Port Holdings, feel that private companies are bearing significant financial costs without reaping adequate rewards. If private companies are expected to continue to seek security innovations, governments must provide increased incentives to do so, and must work to make the costs of security as widespread as the macroeconomic benefits of secure trade.

In addition to the commonalities mentioned above, port interviews revealed security issues and procedures that are unique to individual nations and ports. The most startling observation in the Brazilian chapter is the dire financial situation of Brazil's port industry; more specifically, overall port operations. Of the $101.3 million promised by the Brazilian government to the national port authority in 2005, only $13.9 million was actually received. Reliance on government funding has prevented the implementation of many security upgrades; at present, ISPS is the only program that has received funding. However, implementation of ISPS has been extremely uneven across Brazilian ports. Brazil was the only country in our study that had yet to achieve full implementation of ISPS standards. Currently, 91 of the 218 port facilities are not fully compliant with ISPS, including the nation's largest port, Santos.

Hong Kong and India are both notable for their technological innovations in port security, and yet both nations still face significant security issues that threaten to undermine their progress. Hong Kong terminal operators have undoubtedly implemented some of the most sophisticated security technology in the world. The ICIS pilot project that allows for 100% screening of container shipments represents a leap forward for global supply-chain security. With the implementation of the ICIS system, the need for a widespread port shutdown after a terrorist threat or incident could potentially be eliminated. Governments and supply-chain participants would be able to track a threatening shipment's movements from beginning to end, and create a targeted shutdown of the necessary areas and facilities. However, lack of widespread government cooperation and coordination on this project could threaten the enormous potential of this technology. At present, governments have yet to establish uniform security protocols that mandate how they will respond and react should the screening exercise uncover a suspicious shipment. Hong Kong is also grappling with a lack of integration between its security procedures and those of mainland China. Presently, over 70% of Chinese exports exit through the Port of Hong Kong. However, most of the goods are moved through mid-stream and river terminals which are not required to be ISPS compliant. Although China and Hong Kong are moving towards better harmonization of their standards, this lack of uniformity presents a major obstacle to the security of Hong Kong trade.

India has also made significant technological strides in its port security. The NSICT terminal at the Port of Jawaharlal Nehru is the first fully automated terminal facility in India. The terminal's NAVIS system uses Radio Frequency Identification allowing operators to track each container's precise movements throughout the terminal. Containers are tracked in real time, creating the ability to identify when, where, and by whom a container is moved. However, the technological innovations of India's new terminal facilities are hindered by uneven technological capabilities across the country and among private companies. At present, over 40% of Indian importers are unable to comply with India's electronic Customs procedures due to a lack of requisite technology.

Veracruz, Rotterdam, Marseille and Durban all share security difficulties caused by the close proximity of port facilities to their city centers. Veracruz has worked to improve port security by subjecting 100% of inbound cargo to gamma-ray screening. However, officials acknowledge that only 10-12% of the captured images are actually inspected. Rotterdam has made significant advances through its creation of a Port Facility Security Toolkit. The toolkit is an automated program that facilitates ISPS compliance through the creation of individual risk assessments and security plans. The program can be adapted to country or port-specific guidelines, and helps to ensure a faster and more uniform implementation of ISPS procedures. Rotterdam's success with the toolkit has led over 30 different nations to implement the software.

South Africa expressed perhaps the greatest willingness to participate in this study and to learn from international security initiatives. However, the country has struggled with the rapid and complete transformation of its security capabilities. Officials expressed great frustration with ISPS' lack of specificity. At the time of implementation, South Africa had few port officials with the necessary expertise and experience to lead an immense

security overhaul. Planners were largely creating security procedures and organizations from the ground up without adequate international guidance. Officials stressed that it is especially difficult for developing countries to marshal the economic resources and manpower required to achieve international compliance. They suggested that international assistance with training and funding would make developing nations much more likely to comply with international standards.

In order to better secure and facilitate global trade, governments must work together to bring about an efficient and harmonized security regime. The proliferation of new security programs should be slowed or stopped until the context into which existing initiatives fits can be better understood and uniformly implemented worldwide.

Chapter 1. Primer

Securing ports and global supply chains has become a priority to governments worldwide, international organizations, and the international trade community. The ever-evolving global maritime security strategy is a mosaic of diverse but theoretically complimentary initiatives. This chapter details the roles and interactions of key government agencies and international organizations, the security initiatives for which they are responsible, and the various ways in which the private sector contributes to and participates in security processes.

United States Port and Supply-Chain Security Overview

U.S. Government Agencies with Security Responsibilities

This section provides a brief introduction to some of the major U.S. agencies involved in national security efforts and a summary of their roles.

U.S. Customs and Border Protection (CBP)

U.S. Customs and Border Protection (CBP) is the federal agency charged with the protection of the Nation's borders. CBP was created on March 1, 2003 and falls under the Department of Homeland Security. With an annual budget in excess of $7.5 billion[*] and more than 41,000 employees, its mission is to prevent terrorism without hampering free trade or travel. One of CBP's primary goals is to "push the Nation's zone of security outward" by partnering with foreign countries and the private sector to enhance overall security. To this end, CBP administers several security initiatives which will be discussed in greater detail in the U.S. Initiatives section.[15]

U.S. Coast Guard (USCG)

The U.S. Coast Guard operates under the Department of Homeland Security and is charged with maintaining and enforcing maritime security along the Nation's coast and outward. Its mission is "to protect the public, the environment, and economic interests - in the Nation's ports and waterways, along the coast, on international waters, or in any maritime region as required to support national security."[16] Approximately 39,000 active duty members and 8,100 reservists carry out the Coast Guard's five operating goals which include maritime safety, protection of natural resources, mobility, maritime security and national defense.[17]

[*] Unless otherwise noted, all currency is listed in U.S. dollars.

Maritime Administration (MARAD)

The Maritime Administration of the U.S. Department of Transportation manages domestic waterway transportation security within the boundaries of the U.S. Its mission is "to strengthen the U.S. maritime transportation system - including infrastructure, industry and labor - to meet the economic and security needs of the Nation."[18] MARAD's strategic objectives are to improve commercial mobility, enhance national security, and promote environmentally friendly maritime operations. MARAD's port security branch "works towards the prevention of international destruction, loss or damage to port assets due to terrorism or sabotage."[19] One of its goals is for the nation to be able to use the merchant marine in times of war or national emergencies as a naval and military auxiliary.[20]

Transportation Security Administration (TSA)

The Transportation Security Administration was created in response to the 9/11 attacks and operates under the Department of Homeland Security. TSA's mission is to "protect the Nation's transportation systems to ensure freedom of movement for people and commerce."[21] While most people are familiar with TSA's air-traffic security initiatives including the Federal Air Marshall Program and aviation security screening,[22] it is actually involved in maritime security as well. TSA, for example, is responsible for the maritime sector's Transportation Worker Identification Credential (TWIC) prototype which will be discussed in greater detail in the U.S. Initiatives section.

National Targeting Center (NTC)

The National Targeting Center was created in November 2001, and operates under the Department of Homeland Security. Its primary functions are to analyze threats to national security and supply CBP with information for the purpose of preventing terrorism. The NTC has 40 permanent staff members working as targeters and analysts. The NTC collaborates and shares information with several agencies including the Federal Bureau of Investigation, U.S. Coast Guard, the Transportation Security Administration, and the Department of Energy.[23]

Bureau of Industry and Security (BIS)

The Bureau of Industry and Security is an agency of the U.S. Department of Commerce which deals with national security issues and high technology. The mission of the BIS is to "advance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership."[24] Some of the functions of the BIS include regulating the export of sensitive goods and technologies; enforcing export control, public safety and anti-boycott laws; assisting with international arms control agreements and promoting public-private partnerships to protect critical national infrastructures.[25] The BIS is the oversight agency for the new Deemed Export Advisory Agency which will be discussed in greater detail in the next section.

U.S. Private-Sector Involvement in Security

The private sector has a vested interest in proposed security initiatives because of the costs of implementation and the various benefits that firms may receive. The varied roles of the private sector in U.S. security processes range from serving as members on advisory committees to public agencies, to security analyses and evaluations performed by consulting firms, to specific proposals made by trade associations and individual firms for securing supply chains. While innumerable examples exist, this section highlights a select few that are illustrative of private-sector involvement in U.S. maritime security activities.

Commercial Operations Advisory Committee (COAC)

The Commercial Operations Advisory Committee was formed in the 1980s to represent importers, customs brokers, carriers and port authorities. It is composed of 20 members that provide advice and recommendations to the Department of the Treasury and the Department of Homeland Security on trade and supply-chain issues.[26]

Deemed Export Advisory Committee (DEAC)

The creation of the Deemed Export Advisory Committee was announced on May 22, 2006, by the U.S. Department of Commerce's Bureau of Industry and Security. The purpose of the Committee is to review existing U.S. policy on deemed exports and to determine whether changes should be made. The DEAC was conceived of in response to increasing concerns of several parties, including the optics and photonics communities, about the recommendations and proposed changes, made by the Office of the Inspector General, on deemed export security. The DEAC will facilitate an informed, yet independent, review that will take into account the needs and preferences of the private sector in determining best security practices for deemed exports. The Committee will consist of a maximum of 12 people drawn from academia, industry and elsewhere.[27]

National Industrial Transportation League (NITL)

The National Industrial Transportation League was formed in 1907 to represent shippers, in matters involving regulatory commissions or agencies. All member companies involved in the transportation of freight (at any point in the supply chain) are eligible to vote in the League. In February 2005, the NITL announced the creation of its new Select Committee on Security (SCS). Its mission is to "serve as a primary resource in developing recommendations for the League on current and new security programs/plans as well as to advance positions which will make [NITL's] domestic and international supply chains safer."[28] Members of the SCS include chairpersons (and each of their committee designees) from each of the NITL's "modal" (Air, Domestic Waterways, Highway, Ocean and Rail Transportation) committees as well as those from the Information Technology Advancement (ITAC), Hazardous Materials (HAZMAT) and Executive committees.[29]

IBM Initiative: Intelligent Trade Lane

Global Movement Management is a supply-chain security initiative under development by IBM Corporation. *Intelligent Trade Lane*, one part of the larger initiative, is a wireless supply-chain security platform developed by IBM and ocean shipper Maersk Logistics which is being marketed as the "Commercial Solution for Real-Time Container Management."[30] Intelligent Trade Lane was designed to provide security and supply chain efficiencies. The technology combines elements such as wireless sensors that determine location and temperature with tamper proof smart cards, and a medium for worldwide communications through cellular, satellite and wireless networks. It is scheduled to be available in fall 2006.[31]

Deloitte Study

Deloitte Touche Tohmatsu, an international auditing and consulting firm, has been working to disseminate security-related information about the private sector's growing focus on security. In September 2004, the company released a study entitled "Prospering in a Secure Economy," which outlines the current challenges faced by private firms in securing different aspects of their supply chains, and provides estimates of the costs of implementing various initiatives. To comply with the Nation's security initiatives, companies must spend money on updating business plans, purchasing new technologies, higher insurance premiums, additional workers and building new infrastructure. For these firms, the cost of security is determined by whatever measures are necessary to ensure a continuous business flow regardless of the type or magnitude of the incident.

Estimated Costs of Selected Security Initiatives, as reported in Deloitte's 2004 Study:

Regulation	**Estimated Cost to Private Sector**
Maritime Transportation Security Act of 2002	$833 million/year $7.244 billion Total (2003 to 2012)
24 Hour Rule (U.S.)	$282 million/year
International Ship and Port Facility Security Code (ISPS)	$1.28 billion up front $730 million/year
Required Advanced Electronic Presentation of Cargo Information	$91 million

While the report encourages private-sector firms to continue to manage and incorporate security procedures into their business plans, it also asks that the government share pertinent security information with the private sector, provide incentives for the private sector to invest in security, and promote global cooperation on standards.[32]

U.S. Government Security Initiatives

This section of the primer outlines the various U.S. initiatives in place to ensure national port and supply-chain security. U.S. policies on port security involve planning for protection and mitigation, planning for response and recovery, identifying and repairing gaps in international supply chains, and using advances in technology to achieve these goals.[33]

Maritime Transportation Security Act (MTSA)

The Maritime Transportation Security Act was signed into law* on November 25, 2002 and "sets out broad guidelines for securing the nation's ports and related intermodal facilities."[34] Developed by the Department of Homeland Security and the Department of Transportation's Maritime Administration, MTSA outlines mandatory requirements that ships and port facilities must follow. The requirements include the development and implementation of security plans, identification of at-risk vessels and U.S. facilities, use of personnel identification cards, placement of automatic identification systems on vessels in U.S. waters and the creation of port committees to coordinate activities among port stakeholders. MTSA security regulations focus primarily on the sectors of the maritime community considered to be at higher risk for security breaches including large passenger vessels, dangerous cargo terminals and offshore oil and gas platforms.[35] The U.S. Coast Guard is responsible for enforcing MTSA.[36]

MTSA is the U.S.' version of the International Ship and Port Facility Security Code (ISPS) and was actually the catalyst for the creation of ISPS, which was fully implemented on July 1, 2004. The main difference between the domestic and international codes is that both Parts A and B of MTSA are mandatory while in the ISPS code, Part B is voluntary. The U.S. Coast Guard is also responsible for the enforcement of ISPS within the United States. ISPS will be discussed in greater detail under the International Initiatives section.

Customs-Trade Partnership Against Terrorism (C-TPAT)

The Customs-Trade Partnership Against Terrorism is a security initiative administered by U.S. Customs and Border Patrol (CBP). C-TPAT is a voluntary government/private-sector partnership, designed to strengthen supply-chain security.[37] A supply chain is defined as the "network of retailers, distributors, transporters, storage facilities and suppliers that participate in the sale, delivery and production of a particular product."[38]

In order for firms to gain membership to C-TPAT, they must meet certain requirements and be certified and validated by CBP. These requirements have rolled out in phases. On March 25, 2005, security criteria for importers were released. On March 01, 2006, C-TPAT criteria for sea carriers became effective; and, on March 13, 2006, the criteria for U.S./Canada and U.S./Mexico highway carriers became effective.

---

* The Maritime Transportation Security Act is now Public Law 107-295.

As of March 2006, there were 10,343 members participating in C-TPAT. Members are classified according to the C-TPAT Tier (I, II or III) which they have achieved. Each tier in the program has corresponding benefits. Tier III members experience the greatest benefits, including a reduced number of CBP inspections and priority inspections through Customs.[39]

Container Security Initiative (CSI)

- The Container Security Initiative was announced in January 2002 as an initiative of CBP. Designed in keeping with the post 9/11 effort to extend the U.S. zone of security outward so that American borders are the last line of defense, not the first, its goal is to prevent a container carrying a high-risk item, such as a dirty bomb, from entering the United States. CSI consists of four core elements:

- High-risk containers are identified using targeting tools, advance information and strategic intelligence;

- Containers are prescreened and evaluated prior to shipment as early in the supply chain as possible;

- High-risk containers are prescreened rapidly using technologies such as large-scale x-ray, gamma-ray machines and radiation devices; and

- Containers that have been tampered with during transit are identified using smarter, more secure technologies.[40]

- Under CSI, U.S. Customs officials are stationed at foreign ports in order to help target U.S.-bound cargo for screening.[41] U.S. Customs officials are currently stationed in 44 CSI-compliant ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America. CSI is designed to be a reciprocal program, inviting other countries to send their Customs officials to U.S. ports in order to target cargo destined for their countries. Currently, only Japanese and Canadian Customs officers are permanently stationed in U.S. ports under CSI.

The 24-Hour Rule

In summer 2002, the U.S. Congress proposed that a new rule be written into the MTSA. As amended by the Trade Act of 2002, P.L. 107-296, the 24-hour rule was finalized in December 2003.[42] The rule requires all sea carriers and non-vessel operating common carriers (NVOCC), except break-bulk carriers and approved break-bulk cargo, to provide U.S. Customs with advance manifest information on cargo bound for the United States at least 24 hours before cargo is loaded on a ship at a foreign port. The manifest includes such information as the contents of the shipment and the identity of the importer.[43] Cargoes with vague descriptions of contents such as “Freight-All-Kinds” and “General Merchandise” are no longer allowed to be loaded on U.S.-bound ships. The primary goal

is to facilitate the identification of high-risk containers prior to arrival in United States waters[44].

The 96-Hour Advance Notice of Arrival

The 96-Hour Advance Notice of Arrival states that all vessels must report their arrival in the United States to the Coast Guard at least 96 hours in advance. The rule also requires the submission of crew, passenger and cargo manifest information.[45] The ship's information is then reviewed and analyzed so that the Coast Guard has adequate time to determine which ships require additional attention. The USCG takes additional security precautions with those ships deemed suspicious or potentially dangerous. Such precautions might entail boarding the ship while it is still at sea and/or armed escort during transit to and from certain ports.[46]

Automated Targeting System (ATS)

Data concerning the shipping industry and its patterns are collected through CBP's Automated Manifest System (AMS). The Automated Targeting System is used to sort through AMS data and track anomalies in order to prevent a terrorist attack. CBP developed targeting rules to identify high-risk characteristics and AMS data are filtered using these targeting criteria. Shipments are then given scores; higher scores lead to further scrutiny.[47]

Automated Commercial Environment (ACE)

The Automated Commercial Environment "is the modernized U.S. trade processing system designed to consolidate and automate border processing to significantly enhance border security and foster our nation's economic security through lawful international trade and travel." ACE is designed to make trade processing more effective within the U.S. Through ACE, truckers, carriers, importers and brokers can file their manifests electronically.[48]

Free and Secure Trade Program (FAST)

FAST is a partnership initiative between the United States and Canada and the United States and Mexico "designed to ensure security and safety while enhancing the economic prosperity of each country." The countries are to utilize industry partnerships, supply-chain security, common risk management principles and advanced technology to streamline the process of moving goods across the borders. The goal of FAST is for low-risk shipments to benefit from expedited border processing so that CBP can concentrate its efforts on high or unknown risk shipments. Those that comply with FAST and C-TPAT can take advantage of the "FAST lanes," which are dedicated for the exclusive use of those that are certified, to be able to cross the border faster.[49]

Transportation Worker Identification Credential (TWIC) Prototype

On May 15, 2006, the TSA approved proposed regulations for the Transportation Worker Identification Credential Prototype. The prototype is designed to ensure that any individual posing a security threat does not gain access to U.S. ports. TSA will collect biographic information from all U.S. port workers with access to secure and/or security sensitive areas of vessels and port facilities, as defined by MTSA. Information collected will include, at a minimum, name, date of birth, address, telephone, job title, employer, photo and fingerprints. In addition, background checks will be conducted to look at immigration status, outstanding warrants, and criminal history and check names against terrorist watch lists.

TWIC, which will use a tamper-resistant biometric technology, is expected to cover at least 750,000 workers and will be funded by user fees. Each worker will pay approximately $139 for a card that will be valid for 5 years.[50] Vessels and port facilities will need to integrate TWIC into existing access control systems and day-to-day operations, update security plans and purchase special card readers.

National Strategy for Maritime Security (NSMS)

The National Strategy for Maritime Security "aligns all Federal government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate Federal, State, local and private sector entities."[51] Since 9/11, several strategies to enhance maritime security have been initiated by various federal departments. NSMS consolidates the various programs and initiatives into a unified plan. It promotes the assessment of threats to maritime security, ranging from terrorist threats to the threat of environmental destruction. Strategic objectives are developed within the Strategy to prevent security incidents and to ensure a strong infrastructure is in place in the event of an incident. Finally, strategic actions outlined in NSMS include enhancing international cooperation, promoting a layered security infrastructure and avoiding the disruption of international trade. There are 8 supporting, mutually reinforcing plans in place to achieve this goal:

- National Plan to Achieve Domain Awareness;
- Global Maritime Intelligence Integration Plan;
- Interim Maritime Operational Threat Response Plan;
- International Outreach and Coordination Strategy;
- Maritime Infrastructure Recovery Plan;
- Maritime Transportation System Security Plan;
- Maritime Commerce Security Plan; and

- Domestic Outreach Plan.[52]

U.S. Private-Sector Security Initiatives

Operation Safe Commerce (OSC)

Operation Safe Commerce was launched on November 20, 2002. OSC was conceived of and developed by ports, shippers, and transportation providers but is jointly administered by the U.S. Department of Transportation (DOT) and CBP. The program funds private-sector initiatives that are designed to enhance container security for cargo moving throughout the international transportation system. CBP and DOT utilize the program both to determine current supply-chain vulnerabilities and to test new programs and improved security measures. Following the assessment and testing phases, those methods determined to be *best-practice* are recommended by the program's Executive Steering Committee (ESC) for implementation. The ESC which draws its members from the TSA, DHS, DOC, USCG, Department of Justice, Department of State, and White House, is responsible for project screening, awarding funding and project oversight.[53]

Smart and Secure Trade Lanes Initiative (SST)

Smart and Secure Trade Lanes Initiative (SST), a program of the Strategic Council on Security Technology (SCST), is a supply-chain security initiative, developed and promoted by the trade industry that offers a global security network from point of origin to point of delivery. "SST combines the people, processes, and technologies involved in supply-chain security in a global network for container security."[54] SST utilizes a number of technologies including radio frequency identification (RFID) hardware, tracking and management software, anti-intrusion systems and automated video surveillance. It was designed in compliance with (and complements) C-TPAT, CSI, OSC and parts of ISPS, among other programs.

SST has been operational since October 2002. The initiative is rooted in international standards and based on the Department of Defense's Total Asset Visibility network actively deployed in over 40 countries and at 750 checkpoints worldwide. The International Organization for Standardization (ISO) has selected SST to be the model for refining container security standards. [55]

U.S. Security Legislation

The GreenLane Maritime Cargo Security Act (S. 2459)

Senate Bill 2459, entitled the GreenLane Maritime Cargo Security Act is a companion measure to approved House Resolution 4954, the "SAFE Ports Act." The bill was designed to strengthen cargo security because security initiatives in place following the terrorist attacks were seen as insufficient. It is a strategy designed to facilitate the resumption of trade following a security incident, close vulnerabilities and gaps, and

maintain the efficient flow of legitimate trade.[56] In May 2006, the GreenLane act was approved by the Homeland Security and Governmental Affairs Committee; it is currently being reviewed by three other Senate committees. Once passed, in conjunction with its counterpart SAFE Ports Act, the two would:

- Authorize approximately $800 million for port security;
- Mandate that DHS construct a comprehensive plan for supply-chain security and upgrade the Automated Targeting System;
- Establish a DHS Office of Cargo Security;
- Establish minimum standards for container storage and shipments;
- Create "GreenLane," a new voluntary import security program to allow for expedited treatment to cargo flows through reduced bonding requirements, pre-loading inspections and container security devices use;
- Assess and update C-TPAT requirements and ensure that C-TPAT member validation occurs within at least 6 months;
- Authorize new Operation Safe Commerce grants for "non-intrusive" inspection equipment, physical access control tests, development of an information-sharing network that will collect data from every intermodal transfer point; and
- Complete the international trade data system.[57]

The Security and Accountability for Every (SAFE) Port Act (H.R. 4954)

House Resolution (H.R.) 4954, also known as the Security and Accountability for Every (SAFE) Port Act, was designed to enhance security at the Nation's ports, prevent threats from reaching the U.S., and to track and protect containers en route to the U.S.[58] H.R. 4954 seeks to "codify several existing port security programs as well as requiring the federal government to establish protocols for the resumption of ocean commerce after a terrorist attack, set forth new container security standards and design a new national strategic plan for port security." The bill, although written in December 2005, was introduced during the controversy over Dubai Ports World's bid to acquire terminals at U.S ports in March 2006.[59]

International Port and Supply-Chain Security Overview

International Organizations with Security Responsibilities

The United States recognizes that international cooperation is critical to ensuring safety and security. As such, the U.S. has stationed Customs officials at a number of ports worldwide, and encourages other countries to do the same. The U.S. is a member of the

World Customs Organization (WCO), International Maritime Organization (IMO), International Labor Organization (ILO), International Organization for Standardization (ISO) and the Organization of Economic Cooperation and Development (OECD). This section examines the roles of the WCO, IMO, ILO, ISO, European Union, UNCTAD, OECD and APEC, and their respective relationships to international security.

World Customs Organization (WCO)

The World Customs Organization originated in 1952 and is headquartered in Brussels, Belgium. Its mission is to "enhance the effectiveness and efficiency of Customs administrations."[60] The WCO's 169 member governments account for more than 98% of international trade.[61] Each member has one vote and one representative. The WCO's activities center around making Customs procedures more uniform and include the development of the Harmonized Commodity Description and Coding System and the approval of the revised International Convention on the Simplification and Harmonization of Customs Procedures.[62] The WCO administers the SAFE Framework of Standards to Secure and Facilitate Global Trade, a newly adopted program designed to modernize Customs administrations and implement global supply-chain security. SAFE will be discussed in greater detail in the International Initiatives section.

International Maritime Organization (IMO)

Established in 1948 and headquartered in London, the International Maritime Organization "is the United Nations' specialized agency responsible for improving maritime safety and preventing pollution from ships."[63] The IMO's primary goal is to adopt international regulations to be implemented and followed by all shipping nations. Safety is the IMO's first priority and one of its most noteworthy tasks as an organization was to adopt a new version of the International Convention for the Safety of Life at Sea (SOLAS) in 1960. More than 40 maritime conventions and protocols have been adopted by the IMO. There are 163 member nations in the IMO and three associate members. IMO costs are shared by the members according to the size of the respective nations' fleets. In 2006, the IMO's top contributing member states were Panama (18.47%), Liberia (7.72%), Bahamas (5.03%), U.K. (4.64%), Greece (4.34%), Singapore (4.02%), Japan (3.76%), Marshall Islands (3.58%), U.S. (3.44%), and China (3.34%).[64] In 2002, the IMO adopted the International Ship and Port Facility Security Code (ISPS), which is an addition to SOLAS, based on the U.S.' Maritime Transportation Security Act, and will be discussed in greater detail in the International Initiatives Section.[65]

International Labor Organization (ILO)

The International Labor Organization is a specialized agency of the U.N. consisting of 178 member countries, which "seeks the promotion of social justice and internationally recognized human and labor rights," Founded in 1919 under the Treaty of Versailles, the ILO serves to develop and adopt minimum standards for international labor concerning freedom of association, the right to organize, collective bargaining, abolition of forced labor, and equality of opportunity and treatment. The ILO also provides technical assistance to its members in such areas as vocational training, labor law and industrial

relations, employment policy, etc. It operates as a tripartite agency in which governments, workers, and employers participate as equal partners. The ILO's three major bodies are the International Labor Conference (an annual conference in which each member state is represented by a worker and employer delegate); the Governing Body (ILO's executive council composed of 14 employers and 14 workers, responsible for policy adoption, the Programme and the budget); and the International Labor Office (the permanent secretariat of the ILO acts as a research and documentation centre and printing house).[66] In 2003, the ILO adopted the Seafarer's Identity Documents Convention (Revised) which will be discussed in greater detail in the net section.

International Organization for Standardization (ISO)

The International Organization for Standardization was founded in 1947 and serves to develop standards for products, corporate processes and industries. While the standards adopted by the ISO are classified as "voluntary industry agreements,"[67] regulations and treaties written by governments and international organizations can mandate the agreements for businesses, if desired. The ISO is a network comprising the national standards agencies of 156 member bodies but, unlike many other international organizations whose membership is uniquely composed of member governments, the ISO also has private-sector members that have come out of national partnerships of industry organizations.[68] Because of its unique makeup, the ISO has great potential to serve as an oversight organization for international government/private partnerships. Financing for the ISO comes from the sale of standards, and member subscriptions determined by the member-nation's Gross National Income and trade figures. Since its inception, the ISO has published more than 15,000 international standards ranging from standards for agriculture and construction to digital coding for multimedia applications. In November 2005, the ISO published ISO 28000 which is the first of a series of standards on supply-chain security outlining a potential security management system.[69] ISO 28000 will be discussed in greater detail in the next section.

European Union

Following the 2004 terrorist attacks in Madrid and 2005 attacks in London, the European Commission was tasked with developing a number of security proposals, including one that would strengthen security measures in ships and harbors. The European Commission (EC), the European Union's Executive governing body, developed a framework to enhance port security proposing that ports:

- Carry out a security assessment in order to determine necessary security measures;
- Develop a port security plan which outlines all measures and details for enhancing port security;
- Nominate a port security officer responsible for coordinating security measures;

- Identify a security authority to supervise security measures and establish the links between political level and security measures on the ground; and

- Establish different security levels.[70]

Additionally, the EC is working on a proposal for a regulation on supply-chain security in the form of an amendment to the current Community Customs Code (Regulation 2454/93). One of the most important provisions in the amendment proposes that EU Customs agencies collect and prescreen shipping manifests, and establishes an Authorised Economic Operator (AEO) program,* similar to the U.S.' C-TPAT program.[71]

On April 22, 2004, the EU and the U.S. signed an agreement of cooperation to broaden the 1997 Agreement on Customs Cooperation and Mutual Assistance in Customs Matters[72] to include container security. The agreement aims to harmonize control standards and security arrangements between the EU and the U.S.[73] Two working groups (the EC-U.S. Expert Groups) were also established under the agreement. One is responsible for security standards and the other for trade partnership; both are responsible for determining additional operational elements needed to facilitate increased cooperation.[74]

Organization for Economic Cooperation and Development (OECD)

The OECD is composed of 30 member countries that share "a commitment to democratic government and the market economy."[75] The OECD is best known for its statistics and publications which encompass a variety of economic and social issues. The "Council" is its governing body, which is made up of member-country representatives who provide guidance on the work of OECD committees. Peer review is widely used and defines the nature of the OECD and its influence is used to gain the adoption of certain public policies worldwide.[76]

The OECD has published a number of reports on maritime security in different countries including the U.S. The organization also conducts workshops in which different countries present their ideas on and procedures for maritime security. The U.S. has used these workshops to facilitate dialogues about maritime security issues and to receive feedback from other countries about proposed initiatives.

The United Nations Conference on Trade and Development (UNCTAD)

The United Nations Conference on Trade and Development was established in 1964. Its mission is to promote "the development-friendly integration of developing countries into the world economy."[77] UNCTAD works to ensure sustainable development in both domestic and international policy. In order to effectively realize its mission, UNCTAD serves three primary functions. It serves as a forum for intergovernmental debate,

* The EU's Authorised Economic Operator program will be discussed in greater detail in the next section.

dialogue and consensus building; acts as a research and analysis unit collecting data for its member governments; and provides technical aid to developing countries and economies in transition. Currently, UNCTAD consists of 192 member governments.

As the "focal point for the integrated treatment of trade and development," UNCTAD often works in conjunction with other agencies and international bodies, both offering assistance and collaborating on various initiatives. For example, UNCTAD works closely with the World Trade Organization in an effort to increase the effectiveness and efficiency of multilateral trade. A Memorandum of Understanding was signed by the two organizations in 2003 which provides for continued collaboration and cooperation on select joint studies and initiatives.

UNCTAD recently released a report which proposes a new approach to maritime transport security that would place the focus on securing the entire supply chain, rather than the industry's current approach which concentrates on securing individual facilities.[78]

Asia-Pacific Economic Cooperation (APEC)

The Asia-Pacific Economic Cooperation (APEC) is an intergovernmental economic forum comprising 21 member economies from the Asia-Pacific rim. The forum aims to promote trade liberalization, business facilitation and economic growth in participating nations. APEC works to facilitate maritime security through encouraging public-private security partnerships, as well as through its ISPS Implementation Assistance Program, which provides assistance to member countries for ISPS implementation.[79]

International Security Initiatives

The International Ship and Port Facility Security Code, the ISO standards, and the WCO Framework of Standards are just a few of the international initiatives in place affecting players involved in maritime security on a global scale. In addition to these and U.S. initiatives, several other countries and communities, have undertaken their own maritime security initiatives, such as the Authorised Economic Operator* program in Europe and the Intermodal Container Inspection System (ICIS) in Hong Kong.

International Ship and Port Facility Security Code (ISPS)

The ISPS code is "a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States." ISPS is based on the U.S.' Maritime Transportation Security Act (MTSA), an amendment to the 1936 Merchant Marine Act. The MTSA was designed to protect U.S. ports and waterways from terrorist attack. Adopted in 2002, ISPS is an amendment to the International Convention of Safety of Life

* The EU's Authorised Economic Operator Program is a separate initiative from the WCO's Authorized Economic Operator Programme.

at Sea (SOLAS) and is administered by the IMO. Part A of ISPS is mandatory and contains security requirements for governments, shipping companies and port authorities. Part B is voluntary comprising a series of guidelines for meeting the requirements in part A. Legally, contracting governments to SOLAS must comply with ISPS.[80]

International Organization for Standardization (ISO) 28000, 28001

ISO 28000: *Specification for Security Management Systems for the Supply Chain* "specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. These aspects include, but are not limited to, financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations."[81] ISO 28000 applies to all organizations regardless of size and/or function within the production or supply chain. Fourteen countries, international organizations (including the IMO and WCO), regional bodies and technical staff from the ISO collaborated to create ISO 28000. [82]

"ISO/PAS 28001: *Ships and Marine Technology - Best Practices for Custody in Supply Chain Security* will assist the shipping industry in meeting best practices as outlined in the World Customs Organization's Framework of Standards. It is expected to be published in the second quarter of 2006."[83]

SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE)

The WCO's SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE) was created in order to help secure the international supply chain. The WCO considers the Customs administrations of different governments to be the key to strengthening global trade security because of their unique powers to inspect cargo, refuse entry and exit and expedite entry. [84] While SAFE recognizes these unique powers, it also encourages international Customs administrations to develop working relationships and engage in collaborative efforts with other government agencies. SAFE, in essence, sets forth the idea that "there should be one set of international Customs standards developed by the WCO that does not duplicate or contradict other intergovernmental requirements."[85]

The four core elements of the SAFE Framework are as follows:

- Harmonize advance cargo information requirements on inbound, outbound and transit shipments;

- Each country that joins the Framework commits to employ a consistent risk management approach to address security threats;

- At the request of a receiving nation, the sending nation's Customs administration will perform an outbound inspection of high-risk containers and cargo; and

- Customs will provide benefits (as defined by SAFE) to businesses that meet minimal supply chain security standards and best practices.[86]

Authorised Economic Operator (AEO) Program

An Authorised Economic Operator (AEO) is a private company that complies with Customs' security requirements and is expedited through Customs procedures in the European Union. Each of the 25 EU countries is responsible for certifying its companies as AEOs, which will equally be recognized by the other EU countries. The AEO is the European Union's version of C-TPAT's "trusted accounts,"[87] although there are key differences between the two programs.

The AEO program is similar to C-TPAT in that the company must file data in advance of cargo arrival, and one of the main benefits is the expedited treatment of cargo. The differences between the two programs are that AEO addresses trade facilitation in addition to security issues, the AEO program requires advance information on cargo that is leaving the EU territory, and there are two separate certificates that an AEO can acquire. One certificate is for compliance with security protocols and the other is for certification with trade regulations. An AEO can choose whether to become certified for security matters, trade or both.[88]

International Private-Sector Security Initiatives

Integrated Container Inspection System (ICIS)

The Integrated Container Inspection System is being tested in a private-sector pilot project currently under way in Hong Kong. Developed with Science Applications International Corporation (SAIC), the ICIS is designed to help Customs agents and other port officials identify high-risk containers as quickly and efficiently as possible without impeding the flow of traffic. The system uses a combination of gamma-ray imaging, radiation technology and optical character recognition (OCR) technologies which allows for the rapid scanning of closed, moving containers in order to detect radiation and/or other potential weapons. The ICIS server then assembles the images collected which are ultimately viewed in a single, integrated display on the ICIS viewer. In addition to being able to screen both moving and stationary containers, ICIS enhances the efficiency of terminal operations by eliminating the need to transport containers to a dedicated scanning area and by automating the container identification/ process at terminal gates.

The Hong Kong Container Terminal Operators Association (HKCTOA) began the pilot project in 2004 in an effort to determine additional security measures for container security in addition to those already mandated by the ISPS code.[89]

Strategic Council on Security Technology (SCST)

The Strategic Council on Security Technology is an international assembly of top executives from the world's largest port terminal operators, major logistics technology providers, retired senior general and flag officers, former public officials and prominent

transportation consultancies. It includes such companies as Hutchison Port Holdings, P&O Ports, PSA Corporation, Savi Technology as well as experts from the security field. The SCST is committed to "helping ensure greater intermodal supply-chain security through best-of-breed practices and technologies while working with a variety of other industry associations."[90] In July 2002, the SCST announced its Smart and Secure Trade Lanes Initiative (SST), which was discussed in detail in the U.S. Initiatives Section.

Chapter 2. International Ship and Port Facility Security Code (ISPS)

Introduction

The International Ship and Port Facility Security Code (ISPS) was adopted in December 2002 as part of chapter XI-2 of the International Maritime Organization's (IMO) Safety of Life at Sea Convention (SOLAS). It was put into effect on July 1, 2004. ISPS is based on the U.S.' Maritime Transportation Security Act (MTSA), an amendment to the 1936 Merchant Marine Act. The MTSA was designed to protect U.S. ports and waterways from terrorist attacks and was signed into law in November 2002. ISPS, operating as an international counterpart to the MTSA, establishes a baseline requirement for the 159 contracting governments to the SOLAS Convention. It provides a common international framework with which to assess security vulnerabilities and threats, implement security measures, respond to security incidents, and facilitate international cooperation.[91] The first section of this chapter provides background information on ISPS, followed by a discussion of its structure and key provisions; the implementation of ISPS in the U.S. and abroad; and recommendations to improve upon current security initiatives.

Background of ISPS

Creation and Adoption of ISPS

Increasing global interdependence and international conflicts have forced the U.S. to become more cognizant of the risks of a terrorist attack on the maritime industry. Leaders and security officials have warned of the potentially devastating effects such an attack could have on the economy and on the safety of civilians. Prior to 9/11, only 2% of containers entering the U.S. were inspected.[92] The international trade community depended heavily on the maritime industry to secure port facilities and ships. In November 2001, the International Maritime Organization resolved to develop new measures for adoption by participating governments for the Safety of Life at Sea Convention. These were adopted in December 2003. In February 2002, the U.S. Congress began working on legislation that would become the Maritime Transportation Security Act. Simultaneously, U.S. delegates to the IMO proposed a similar initiative (based on MTSA but to be implemented on an international scale) to the IMO's Maritime Safety Committee. Following some initial hesitation, this proposal was largely incorporated into ISPS, which was approved on December 13, 2002.[93]

ISPS was adopted to create security standards for port facilities and the international maritime industry. ISPS provides a "standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities."[94] ISPS is divided into two sections: Part A consists of mandatory regulations delineating the basic responsibilities for governments, port

authorities, and shipping companies while Part B provides voluntary guidelines on how to meet those requirements.[95]

Participation in ISPS is not limited to governments; rather, ISPS requires cooperation and coordination between "contracting governments, government agencies, local administrations, and the shipping and port industries."[96] More than 159 countries must comply with the regulations put forth by the 2002 amendments.[97] Additionally, both SOLAS vessels weighing more than 500 gross tons traveling internationally and their landing ports are subject to the ISPS regulations.[98]

ISPS in the United States

The U.S. Coast Guard is charged with enforcing the Maritime Transportation Security Act in the United States.[99] The Coast Guard must review and approve security plans proposed by SOLAS member-country seaports, waterfront terminals and specified vessels.[100] MTSA also requires the "designation of Coast Guard officials as local-area Federal Maritime Security Coordinators… [and] directs the Secretary of DHS to establish a Coast Guard maritime safety and security team."[101] The Coast Guard's duties also include targeting vessels that have recently visited a country that is not ISPS compliant. As of June 2005, five countries remained non-compliant: the Democratic Republic of Congo, Guinea-Bissau, Liberia, Mauritania and Nauru.[102]

Structure of ISPS

ISPS, Part A

The regulations delineated in Part A, are mandatory for all SOLAS countries. ISPS specifies standards for ships and for port facilities. Passenger ships, cargo ships, and mobile offshore drilling units participating in international trips are also subject to the code.[103] ISPS sets forth the responsibilities of the contracting governments, ships and shipping companies, and port facility owners/operators. Contracting governments can delegate some responsibilities to a recognized security organization (RSO).[*] Contracting governments are responsible for establishing security levels that provide guidance to stakeholders on security threats and dictate measures that must be taken at each one. The security levels prescribed by ISPS are:

> *Level 1*: the level for which minimum appropriate protective security measures shall be maintained at all times;

[*] According to U.S. Coast Guard RSO Targeting Guidelines, accessed on August 31, 2006 at http://www.uscg.mil/hq/g-m/pscweb/RSO.htm, a "Recognized Security Organization (RSO) is an organization with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized to carry out an assessment, or a verification, or an approval or a certification activity, required by Chapter XI-2 or by Part A of the ISPS Code."

Level 2: the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident; and

Level 3: the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable or imminent, although it may not be possible to identify the specific target.[104]

ISPS ship requirements include:

- *Ship Security Assessment:* includes evaluation of current security measures, key shipboard operations, possible threats and weaknesses;[105]

- *Ship Security Plan*: "developed to ensure the application of measures on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident;"

- *Ship Security Officers*: "person(s) on board the ship, accountable to the master,…responsible for the security of the ship;"

- *Company Security Officers*: "the person(s) designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained;"

- *Records*: appropriate records should be kept of "training, drills and exercises; security threats and security incidents; breaches of security; changes in security level; communications relating to the direct security of the ship;"[106]

- *Training, Drills and Exercises*: all ship personnel shall have appropriate knowledge; drills will be practiced at regular intervals;[107] and

- *Verification*: after the ship has gone through its verification process, it shall receive an International Ship Security Certificate to be used convey identity information to receiving ports.[108] This information must be transmitted to the appropriate U.S. authorities 96 hours before landing at U.S. ports.[109]

ISPS also applies to all facilities that serve ships listed in the section above.[110] The facilities' requirements include:

- *Port Facility Security Plan:* "a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident;"

- *Port Facility Security Officer:* "the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan;" and

- *Training, Drills, and Exercises:* all facility personnel shall have appropriate knowledge; drills will be practiced at regular intervals.[111]

Both vessels and facilities must monitor and control access, observe people and cargo, and ensure that security plans are both realistic and feasible.[112]

ISPS, Part B

Part B is designed to provide broad guidelines that will help vessels and facilities satisfy the regulations defined in Part A. Participation in Part B is voluntary.[113] Part B states that the facility security plan should provide what measures should be taken at levels one, two and three. The facility should be prepared to operate at each security level.[114] ISPS sets forth a like expectation for vessels.[115]

Maritime Transportation Security Act (MTSA)

MTSA was signed into law on November 25, 2002. It is the domestic component of U.S. efforts to improve maritime security. As the primary inspiration for ISPS, many of MTSA's basic regulations are similar. MTSA, however, applies to more vessels and facilities and makes binding most of the guidelines found in Part B of ISPS. MTSA was fully in effect by July 1, 2004, affecting 10,000 vessels, 5,000 facilities, 361 ports and 40 offshore facilities.[116]

National and Area Maritime Security

The National Maritime Security Strategy relies on national and regional security plans to ensure proper coordination of national, state, and local agencies with port and vessel operators. The U.S. Coast Guard (USCG) is the primary Department of Homeland Security (DHS) agency responsible for developing the national plan. MTSA requires the plan to contain the following elements:

- Procedures for preventing a national transportation security incident;
- Procedures for restoring cargo flow in U.S. ports after security incidents;
- Assignment of federal maritime security roles;
- Procedures for federal coordination with state and local governments;
- A national system of surveillance and notice;
- Designation of federal maritime security coordinators (FMSC);
- Recognition of secure systems of intermodal transportation; and
- The identification of national resources for maritime security.[117]

The national plan is built upon 45 Area Maritime Security (AMS) plans. Each USCG Captain of the Port (COTP) acts as the security coordinator in his or her respective zone. The COTP has the authority to establish, direct, and appoint members to the AMS committees. Committee members are selected from government agencies, local law enforcement and public safety agencies, the maritime industry, and other port stakeholders.[118] Among the committee's responsibilities are: the identification of critical port infrastructure and operations; recognition of risks; determining mitigating strategies; the assurance of a risk-based port security assessment; and the advising of the COTP in developing the AMS plan and disseminating threat and security information to port stakeholders.[119] The AMS plan must incorporate the following elements:

- Details of operational and physical measures in place at each Maritime Security (MARSEC) level;
- Details of the security incident command and control system;
- Details for reviewing and amending the security plan when necessary;
- Measures to prevent the introduction of dangerous substances and devices into designated restricted areas;
- Measures to prevent unauthorized access to restricted areas;
- Procedures and expected timeframes for responding to security threats and reporting security incidents;
- Measures to maintain information security;
- Procedures to respond to a vessel security alert system within or near the port; and

- The jurisdiction of state and local government and law enforcement agencies. [120]

The COTP and AMS committee are required to coordinate an exercise at least once per calendar year to test the AMS plan.

The Commandant of the USCG, or his designee, can issue MARSEC directives to mandate specific measures for vessels and facilities affected by a security incident.[121] He also sets the security levels, which are aligned with the Homeland Security Advisory Systems, to communicate threat information to the industry and the general public.

The MARSEC levels require specific measures in area and facility security plans. Each COTP can temporarily raise the level within his or her area of responsibility in response to specific and urgent circumstances.[122]

Port Facility Security

In accordance with ISPS requirements, all recognized facility owners or operators are required to designate a Facility Security Officer (FSO). The FSO must ensure that a facility security assessment is conducted and must develop and implement a facility security plan (FSP).[123] The FSP includes the following elements:

- *Security Administration and Organization:* the owner/operator must define the facility's organizational structure and the roles and responsibilities of security personnel. Security personnel must be qualified according to the requirements of 33CFR Part 105.210;

- *Personnel Training:* the plan must outline security training for all personnel at the facility, in compliance with 33CFR Part 105.215. This training includes relevant provisions of the FSP, MARSEC levels, detection of dangerous substances, and common security countermeasures;

- *Drills and Exercises:* the MTSA requires operators to test their security personnel at all MARSEC levels and identify key deficiencies.[124] FSO's must conduct at least one drill every three months and a more comprehensive live or tabletop exercise at least once each calendar year. FSP's must fully describe these drills and exercises and ensure they comply with the requirements of 33CFR Part 105.220;

- *Recordkeeping:* FSO's must keep records of security activities and make them available to the USCG upon request. The security plan must detail the method in which this is done;[125]

- *MARSEC Level Coordination:* the FSP must detail how the facility will respond to different MARSEC levels in compliance with 33CFR part 105.230. The facility has 12 hours to implement required security measures in the case of a change in MARSEC level and to report whether it has complied with the COTP;

- *Communications:* facility security personnel must have redundant systems and procedures in place to communicate with vessels, the COTP, and appropriate national and local authorities. The FSO must detail a system to communicate security information internally as well. In addition, all facility access points must be equipped with a means to communicate with appropriate security responders;

- *Procedures for Interfacing with Vessels:* procedures for interfacing with vessels must be detailed at all MARSEC levels;[126]

- *Declaration of Security (DoS):* a declaration of security, as prescribed by ISPS, is an agreement specifying the security responsibilities between a facility and a vessel during an interface. The FSP must describe how and when the DoS is used;[127]

- *Security Systems and Equipment Maintenance:* the FSP must describe how security systems are tested, maintained, and repaired on a regular basis;

- *Security Measures for Access Control:* the FSP must explain how the owner/operator prevents the introduction of dangerous devices or substances into the port, secures hazardous material within the port, and controls access to the facility land and water. 33CFR part 105.255 outlines requires specific access control measures for each MARSEC level;

- *Security Measures for Restricted Areas:* restricted areas must be identified to protect personnel, key assets, cargo, vessel stores, and vessels. The FSP must identify who has access to these areas at each MARSEC level and a means to enforce and monitor access control measures;[128]

- *Security Measures for Handling Cargo:* measures must be in place to prevent cargo tampering and ensure that all cargo is properly identified for temporary storage, loading onto a specified vessel, or released to a specified carrier. Security procedures should be in place with regular shippers and all dangerous goods must be continuously inventoried. Specific measures are required for each MARSEC level; [129]

- *Security Measures for Delivery of Vessel Stores and Bunkers:* the FSP must deter and prevent tampering with vessel stores through the use of visual and physical examinations, and detection devices. Increased screening frequencies are required for each successive MARSEC level;[130]

- *Security Measures for Monitoring:* the FSP must specify how, at all MARSEC levels, the owner/operator continuously monitors the facility and its approaches, restricted areas, and vessels at the facility. This can be accomplished through lighting, patrols, intrusion-detection devices, and/or other surveillance equipment;[131] and

- *Security Incident Procedures:* in the case of a security breach or incident, the FSO must have procedures in place for each MARSEC level to respond, report, and maintain critical facility operations and vessel interfaces.[132] .

Facility security assessment reports and security plans are initially reviewed by a USCG contractor at the National FSP Review Center in Overland Park, Kansas. The COTP then reviews the plan and gives final approval, which is valid for five years. The FSO is required to audit the FSP annually. Upon approval, the USCG inspection cycle begins, which includes facility inspections and MTSA compliance exams.

Criticism

Several publications have offered criticisms of the newly implemented code. One article argues that MTSA does not address viable security risks. The real threat would come, the article posits, from a small vessel in an attack similar to the one on the U.S.S. Cole.[133] The article also proffers that terrorists would, in reality, do everything in their power to comply with MTSA guidelines, so as to avoid drawing undue attention to themselves and their vessel.[134] While many port security officials feel that MTSA is necessary and valuable, some feel that it has increased their workload by an "unreasonable" amount. They argue that there is now more work to do, given the same time and pay with which to complete it.[135] Reactions to the MTSA are diverse, and one comment may completely discount another: some "felt the strain"[136] and recognized a general "lack of manpower,"[137] stating that they have to "work extra hours and [aren't] paid overtime"[138] and have difficulty remembering all the acronyms,[139] while others remarked that "the code has not really affected the workload [and] has improved security"[140] and that "the administrative side isn't too bad."[141] Although port officials seem unable to reach any kind of consensus, this may be due to the diverse needs of their respective ports. Currently, at-risk ports receive the majority of funding. Smaller ports struggle to implement MTSA with little financial aid.

Funding

The issue regarding the way in which MTSA should be funded is a sensitive one. MTSA is obviously a financial (as well as logistical) burden for ports.[142] Implementing MTSA has been estimated to cost U.S. ports up to $1 billion* annually.[143] The legislation calls for Congress to cover roughly 75% of the costs associated with its implementation. Congress, however, has not met this mandate and ports have been held responsible for finding sources of funding on their own.[144]

Several suggestions have been made with respect to funding. Some suggest that container shippers should pay an additional fee to the ports they are using.[145] This plan could affect ports differently. Ports with higher capacity and traffic would raise more money. Since these are the ports that are most likely to be deemed high-risk, the container-fee plan could accommodate the ports' needs more precisely than a general government grants

* Unless otherwise noted, all currency is listed in U.S. dollars.

system. The shippers in question, however, already pay fees and may be resistant to this proposal.

Another suggestion is that the federal government should pay for implementing MTSA in ports. [146] Proponents of this plan feel that since the code addresses national security, it is in the nation's best interest to ensure that all ports are properly financed and protected.[147] Additionally, a report from the Congressional Research Service states that the maritime industry generates $15 billion dollars in general revenue. Since the industry has already raised this amount of money, the government could direct it back to the ports to fund MTSA.[148]

A third proposal offers that the maritime industry should finance its own port security because "it is a direct beneficiary of improved security as it reduces cargo theft and other economic damages."[149]

Attendees of a 2006 conference on maritime security voiced complaints about how financial aid is distributed among domestic ports. Ports are assessed for possible terrorist threats; DHS then awards monies to high-risk/greater-target ports based on port grant applications. The monies awarded come from Congressional port security grant appropriations. Many port officials reported feeling that their ports had been slighted.[150] Such a structure of awarding only high-risk ports may transfer some threat to smaller ports. If funding enhances a port's security, those ports will be viewed as citadels that cannot be breached. Lower-risk ports, to which less attention is paid anyway, may become the next target. Indeed, there is not enough money to properly finance all ports, but this fact only confirms that the current system of allotting finances must be revisited.

During the conference, Thomas Robison, Director of Transportation and Intermodal Security Division of the Department of Homeland Security, offered advice to those who weren't receiving adequate financing. He suggested that ports would receive better funding if they followed examples of successful budgets, justified all expenditures, demonstrated how their proposal decreased their security risk, and collaborated with neighboring corporations and ports to create joint plans.[151] By following these suggestions, Robison stated, smaller ports may find that they receive more funding and are better able to meet their goals. Today, however, the issue of who should bear the financial burden associated with implementing MTSA is still up for debate.

ISPS Abroad

Compliance

Compliance with ISPS is not mandatory; nor is it even necessarily beneficial to many countries. Most countries believe, however, that in order to maintain their economic vitality (i.e., engage in continued trade with the United States), they must adhere to these procedures. As for ships, one Captain is quoted as saying that the "failure to implement [ISPS] can result in a variety of control actions: detention until they comply, we won't let them unload cargo, or we could kick them out."[152] This chapter will later address the

issue of moving beyond compliance. Unless each country realizes a benefit, it is unclear whether the international trade community can move beyond compliance.

In June 2004, just prior to the implementation of ISPS, the IMO announced that 38 governments had reported issuing 4,841 International Ship Security Certificates. This number constituted a 150% increase over the previous month. However, only 11% of ports had approved plans.[153] Ports and ships were so heavily focused on security that their safety compliance actually declined in 2004. By December 2004, the percentage of vessels arriving in U.S. ports that encountered security problems dropped to 1.5%.[154] As of the beginning of 2006, 36 of the 159[155] contracting governments to SOLAS were found to be in "significant" compliance with ISPS.[156] These 36 have gone above and beyond the requirements of ISPS. Great progress has been made in establishing compliance. Governments clearly made a huge effort to ensure that their ships and ports were properly certified.

Key Points from Case Studies

One aspect of this project involved travel to a number of important maritime ports around the globe both to see firsthand what kinds of security measures were in place and to interview port and government officials responsible for creating and/or enforcing such measures. In the forthcoming chapters, our findings will be presented on a variety of issues, legislation and security measures that we observed and learned of in Brazil, France, Hong Kong, India, Mexico, the Netherlands and South Africa. Below, we have highlighted some of the key findings as they pertain to the implementation of and satisfaction with ISPS in the aforementioned countries.

Whereas each of the *countries* visited have been deemed ISPS compliant by the International Maritime Organization, some of the *individual ports* (including Santos, Brazil) are not yet officially compliant ports. In Brazil, a June 30, 2006 deadline has been set by the Office of Institutional Security of the President of the Republic by which point all Brazilian ports must have achieved full compliance. Full compliance indicates that all provisions set forth in Part A of ISPS must be met, while those outlined in Part B are still considered voluntary. Interestingly, all of the countries involved in this study adhere to most if not all of Part B's stipulations. France and the Netherlands, for example adhere to most provisions under the Directive of the European Union which has mandated parts of Part B for all EU member states. In Mexico, the situation is similar, whereas in Hong Kong most individual terminals have chosen to adhere to Part B. Finally, the federal government of India declared Part B of ISPS to be compulsory for all ports.

During our port visits, we inquired as to the overall level of satisfaction with ISPS in the ports and the answers varied tremendously. While India and the Netherlands reported that no major problems had been encountered either in ISPS' implementation or in overseeing it at the ports, France and South Africa were much more critical of the lack of instructions and guidelines available for implementing ISPS and were particularly

displeased with the complete absence of any harmonization of its implementation or oversight agencies from country to country. Mexico, on the other hand, was pleased with ISPS from start to finish, and seemed happy with ISPS' implementation, which had transformed the way in which security measures were conceived of and implemented in the ports.

Finally, we asked stakeholders both within the foreign governments and working at the ports themselves, to address the issue of financing ISPS in their respective countries and ports. France and South Africa were, once again, in agreement that financing such an initiative had been (and continues to be) almost prohibitively expensive. France in particular was adamant that such an all-encompassing government-led initiative could not simply continue to expect that the private sector would pick up all of the costs associated with implementation and oversight. Private operators in France stressed the need for a more equal division of financing responsibilities to include the state and /or the E.U. South Africa expressed a desire to see a well-funded international organization or body really take control and be responsible for harmonization of the code from country to country and agency to agency. The most interesting findings in terms of financing ISPS came out of Brazil and our case study at the Port of Santos. While ISPS' implementation has become one of the Brazilian federal government's top priorities and funding has been awarded to ports by the government in order to reach full compliance, CODESP, the government entity responsible for implementing ISPS has a current debt of more than $300 million dollars.[157] The Port of Santos, for example, is close to not being able to pay its renegotiated debt service through the federal program Refis. We felt it was important to note the financial situation that CODESP is in, because ISPS and its implementation is one of the few port programs to be executed throughout the country. Now, in the midst of this national effort to become fully compliant by June 30, 2006, many terminals and businesses are claiming they cannot afford the necessary equipment. Container terminal operators have even admitted to passing the costs of implementation onto port users through higher rates.

The diversity of the answers and the overall differences of opinion from country to country only serve to emphasize the importance of harmonization and international standards and highlight the financial and ideological discrepancies in different countries that must be taken into consideration when developing and trying to implement such globally significant legislation and initiatives.

Domestic Success vs. International Success

An article published in an international shipping journal comments on the huge discrepancy between "U.S. and EU ports and those in less developed countries, particularly in African states. Some ship officers talk of a two-tier system at ports around the world, with the U.S. on one level and the rest of the world on another."[158] This is most likely due to differences in resources. As previously mentioned, some officials criticize ISPS because they feel it supports mainly U.S. interests. Other countries are forced into participating out of fears of economic isolation.

The United States seems to display more of a fear of terrorism than do many other countries. Some Western European countries experience more frequent acts of terrorism than the U.S., and yet they still do not consider ISPS to be as necessary as does the U.S. In short, there is absolutely a difference between ISPS in the U.S. and in other countries. However, we cannot definitively say whether the difference stems from resource limitations, a lack of fear of terrorism, or some other unknown cause.

ISPS and Ocean Liners

The World Shipping Council (WSC) represents over forty ocean liner shipping companies. The goal of the organization is to "provide a unified voice for the liner shipping industry in its dealings with policymakers and other industry groups interested in international transportation issues."[159] In a recent trade journal article, Chris Koch, WSC President and CEO, commented on new security initiatives abroad: "it is unclear whether what will result is the objective a uniform, common approach to enhancing security, or the result will be a collection of inconsistent, non-recognizing systems that will become a burden to trade."[160] Koch further elaborated in a follow-up interview that he has no reservations about the intent or implementation of ISPS. He noted that new security initiatives should focus on enhancing risk assessment.[161] This idea will be elaborated upon in the final section of this chapter.

ISPS in the Future

The Importance of Ports

The most likely scenarios for a maritime terrorist act include incidents of seizing a port, attacking a commercial ship, attacking U.S. Navy ships, and using land around a port to attack neighboring facilities.[162]

Such an attack on a U.S. port would have an enormous economic impact. One estimate states that the cost of a port closure "[would be] approximately $1 billion per day for the first five days, rising exponentially thereafter."[163] The maritime industry annually contributes almost $750 billion to the U.S. Gross Domestic Product and constitutes 95% of all overseas trade each year.[164] Maritime ports are equally an integral component of U.S. national security. The Department of Defense uses 17 ports for military deployments. According to the U.S. Government Accountability Office (GAO), if one of these ports were attacked "massive civilian casualties would be sustained, but [the] Department of Defense could also lose precious cargo and time and be forced to rely heavily on its overburdened airlift capabilities."[165]

Standardized ID System

The Transportation Workers Identification Credential (TWIC) program is a proposed identification system that has yet to be approved of or introduced into ports. "The TWIC card will standardize a single common ID card platform, containing at a minimum a digital photo, hologram security layer, a contact chip migrating to a contact and

contactless chip, a magnetic stripe, 2D barcode and a visible TWIC ID number. The chip will store a reference biometric (to be determined) for instant electronic verification, as well as a PKI digital certificate for logical access and electronic signatures."[166]

While some ports are willing to pay to accelerate the adoption process of the TWIC program in their facilities, others believe that it will simply result in an inconsistent identification system due to constantly evolving technologies and continually updated versions of standardized ID systems.[167]

Information-Sharing

The next step in securing the supply chain is constant information-sharing among officials. The GAO reports that "in surface transportation, timely information sharing has been hampered by the lack of standard protocols to exchange information among federal, state, and local government agencies and private entities."[168] Improving information sharing is the first step towards creating truly effective response plans in port facilities.

In the same vein, governments may not currently have enough information to contain a security incident to one region. For instance, the initial response to the attacks of 9/11 was to ground all flights, even though only a few were actually hijacked. In the event of a terrorist attack on the maritime industry, the entire supply chain could be halted.[169] This could quickly escalate from the economic and military consequences outlined earlier to a situation in which citizens could not access the goods they need in order to survive. Officials must gather appropriate and accurate intelligence from participants in the supply chain. With that information in hand, officials can accurately target at-risk vessels and ports, thereby containing potential terrorist incidents to small regions.

Beyond Compliance

Craig Bone of the Department of Homeland Security defines ISPS compliance as conformity and the readiness to conform. The goal of moving beyond compliance entails maintaining the ability to effectively comply with regulations. Moving beyond compliance requires a cultural shift. Instead of focusing on efficiency, ports and ships need to focus on security.[170]

Countries will only comply with ISPS so long as it directly benefits them. One critique mentions that ISPS is beneficial solely to the U.S. and that countries comply because to do otherwise would threaten their economic security.[171] Most countries are concerned about the transport of drugs and contraband, the perpetuation of the black market, and the possibility that a weapon of mass destruction headed for another country might actually detonate en route. International ships and ports may have more incentive to comply if ISPS is amended to address these more pressing concerns.

Lessons Learned and Conclusions

The Maritime Transportation Security Act and the International Ship and Port Facility Security Code were both conceived of in an attempt to better protect the maritime supply

chain against a possible terrorist attack. The goal is to provide a "standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities."[172] ISPS consists of two parts, one mandatory and one voluntary (both are mandatory under MTSA). Part A gives regulations for governments, port authorities and shipping companies. Part B provides guidelines that may aid participants in implementing Part A.

Those involved in the implementation of these recent initiatives have raised concerns about increased workloads, difficulty understanding the code, communication difficulties due to numerous acronyms, and longer hours. Most of these issues will be resolved with time. People will become better acquainted with ISPS and implementation will no longer be a labored process.

Several key issues should be of interest to Congress. There are three ways in which ISPS may be improved upon with further legislation. The first is the successful implementation of a standardized biometric identification card. The second is the improvement of information gathering and sharing in order to target perpetrators without disrupting the entire supply chain. The third is to identify ways in which more countries can realize benefits from ISPS compliance. Once these three modifications have been made, many more countries will move beyond compliance, generating a more secure supply chain.

Chapter 3. Customs-Trade Partnership Against Terrorism (C-TPAT)

Introduction

In December 1993, the U.S. Congress enacted the Customs Modernization Act, calling for "shared responsibility" between U.S. Customs and Border Protection (CBP) and the private sector, specifically importers. The act set forth that both public and private-sector participants have *equal* roles to play in compliance with trade and Customs laws, and legally shifted the responsibility for merchandise declarations to the importer. More importantly, the act established "informed compliance," a process whereby importers' Customs-compliance systems are assessed, rated and revised if necessary to ensure the systems' utmost security and efficiency.[173]

Nearly a decade later, in another effort to combine public and private resources to address the threat of a terrorist attack on the maritime supply chain, the Customs-Trade Partnership Against Terrorism was launched in late 2001. C-TPAT is an "anti-terror partnership [that] seeks to safeguard the world's vibrant trade industry from terrorists, maintaining the economic health of the United States and its neighbors."[174]

Designed with CBP's layered defense strategy in mind, C-TPAT is often touted as the most successful government/private-sector anti-terror program to date. The program aims to enhance the security of the maritime supply chain and encourage cooperative relationships and collaboration between the various private firms, industry groups and government agencies involved in transport.[175] The voluntary program is non-contractual and, in each case, either party (government or private firm) can terminate the agreement at any time via written notice.[176]

C-TPAT Goals

C-TPAT was designed with five primary goals in mind. It aims to:

1. *Ensure that C-TPAT partners improve the security of their respective supply chains pursuant to C-TPAT security criteria*

To this end, CBP supply-chain specialists visit partners, vendors, and vendors' plants to confirm that security practices are reliable and effective. C-TPAT partners must address a broad range of security issues in their supply-chain plans, including personnel security, physical security, access controls, manifest procedures, threat awareness, and document processing. Procedures are then put into place to formalize C-TPAT self-policing and periodic self-assessment. Furthermore, participants are required to "engage and leverage all business partners within their supply chain."[177]

2. Provide incentives and benefits to include expedited processing of C-TPAT shipments to C-TPAT partners

C-TPAT incentives and benefits include a reduced number of inspections and reduced border wait times, access to the Free and Secure Trade (FAST) program when crossing the Canadian and Mexican borders, and invitations to CBP antiterrorism training seminars. A primary benefit of C-TPAT certification offers that, in the event of an incident that disrupts port activity, C-TPAT members' goods will be the first to leave the port again. CBP is planning an additional level of benefits for partners who surpass the highest suggested level of security.* For industry partners, the most appealing potential benefit seems to be the "GreenLane," whereby partners can pass through Customs with significantly reduced inspections. The "GreenLane," however, is dependent on the development of the "smart container" (see goal four) and thus has not yet been realized. Secondary benefits include greater supply-chain integrity, reduced theft, and stronger brand equity.[178]

3. Internationalize the core principles of C-TPAT through cooperation and coordination with the international community

Achieving this goal requires efforts on the part of both the public and private sectors. Domestic firms are now contractually requiring foreign businesses to meet C-TPAT requirements, often calling for regular audits. CBP is working with individual Customs administrations to coordinate anti-terrorism efforts as well as with various international organizations, including the World Customs Organization (WCO), to develop an international framework built upon public-private partnerships.[179]

4. Support other CBP security and facilitation initiatives

C-TPAT works to support the FAST program, the development of a more secure container, and CBP's Container Security Initiative (CSI), in addition to other CBP and DHS anti-terrorism programs. The FAST program is a bilateral initiative, between the United States and Canada, and the United States and Mexico, respectively, that provides expedited cargo-processing for qualifying carriers, importers, and drivers at land borders. In conjunction with CBP's Advanced Container Security Device program, C-TPAT is working to develop and employ the "smart container," a concept that would include high-tech security seals and tamper-resistant devices to maintain container security. C-TPAT is also working with programs such as the Industry Partnership Programs (IPP), Carrier Initiative Program (CIP), Business Anti-Smuggling Coalition (BASC), and the Automated Commercial Environment (ACE).[180]

5. Improve administration of the C-TPAT program

CBP hopes to modernize and expand the C-TPAT program by implementing a human capital plan, expanding the supply-chain specialist (SCS) training program, and

---

* See "New Criteria & Standards" subchapter

enhancing C-TPAT's overall data collection and information-management capabilities. As of 2004, more than 40 SCS positions had been filled. CBP hopes to fill additional positions throughout 2006, while simultaneously expanding the SCS training, perhaps through coordination with universities. C-TPAT is working with the CBP Modernization Office (CBPMO) to collect more substantive information related to C-TPAT security activities.[181]

CTPAT Participants

C-TPAT is currently open to U.S. importers of record, U.S./Canada highway carriers, U.S./Mexico highway carriers, rail carriers, sea carriers, air carriers, U.S. marine port authority/terminal operators, U.S. air-freight consolidators, ocean transportation intermediaries and non-vessel operating common carriers (NVOCC), Mexican manufacturers, certified invited foreign manufacturers, and licensed U.S. Customs brokers.[182] As of March 2006, the C-TPAT program had 10,343 applicants and 5,779 certified members.[*] The FY06 Presidential budget for C-TPAT constituted $42.3 million to "increase supply-chain security and expedite the clearance of legitimate trade."[183]

C-TPAT Participant Status: Tiers I, II and III

There are three statuses or "tiers" for C-TPAT participants. Firms designated as "Tier I" have applied and been accepted, by being "certified," into the program, but have not yet been "validated" (described in the following section). "Tier II" participants have been validated by CBP and "Tier III" participants have been validated and have gone above and beyond CBP requirements and are considered to be using best practices.

The designations for each tier are made by CBP headquarters and each tier has corresponding benefits. Tier III participants receive the greatest benefits. As of March 2006, CBP had designated 139 Tier III firms.[184]

C-TPAT Membership Process

CBP has created a multi-step procedure for C-TPAT applicants. Applicants must first complete a C-TPAT Supply-Chain Security Profile Questionnaire (summarizing the firm's supply-chain security procedures) and submit a signed agreement stating that they wish to participate in the program. The agreement not only outlines a list of security guidelines and additional recommendations[†] that the applicant, in signing, agrees to implement and respect, but it also indicates the applicant's willingness to enhance communication and develop sustainable relationships with supply-chain business partners.[185]

---

[*] C-TPAT's certified membership includes 248 foreign manufacturers, 33 marine ports, 1,297 carriers, 1,080 brokers, and 3,121 importers. Of these, 139 have reached tier 3 status.

[†] Guidelines and recommendations are specific to the category of applicant (i.e., sea carrier, rail carrier, etc.)

Within 60 days of these initial submissions, C-TPAT applicants must electronically submit a more in-depth security profile, the details of which depend on the type of business (i.e., shipper, importer, etc.).[186] Upon receipt of the second security profile, CBP has another 60 days to review it. CBP compares the applicant's profile to standards developed jointly by CBP and the industry. If no weaknesses or gaps in the security profile are found (or after any such weaknesses have been resolved), CBP signs off on the profile and the firm is, heretofore, "certified." The one exception in this process is specific to importers, which must additionally undergo a "vetting" process (described below) before they can begin to enjoy C-TPAT benefits. CBP further encourages firms to conduct annual self-assessments and regularly update their security profiles.[187]

One of the most important, though often overlooked, parts of the C-TPAT application is the provision for "self-policing and record retention." The self-policing plan (which must be written and proposed by the applicant firm) acts as a sort of promissory note to ensure that, once certified as C-TPAT compliant, security plans and programs are actually implemented, security requirements are clearly communicated to other supply-chain members, and records of compliance are maintained by the C-TPAT member.

C-TPAT specialists are trained at headquarters, to make the validation visits to the importers. Although the field visits are to involve only C-TPAT and not other Customs issues, several participants in our survey (described later in this chapter) expressed concern over what appeared to be overreaching on the part of the inspectors into areas beyond validation of the information in the questionnaire.

Additional Security Step for Importers

Rather than comparing the importer's security profile to pre-established standards, the "vetting" process examines the importer's history. CBP consults several data sources in search of evidence of past compliance with Customs laws and regulations, as well as any history of violations. If the importer is given a favorable review, C-TPAT benefits will begin in a matter of weeks. If CBP issues an unfavorable review, however, benefits will only begin if the importer successfully passes the subsequent "validation" process, described below.[188]

The "validation" process is designed to ensure that the firm's security profile and self-assessments are "reliable, accurate, and effective." CBP provides members with 30 days written notice prior to the validation. Together, CBP and the firm determine what portions of the firm's supply chain are to be inspected. CBP officials and firm representatives then perform an on-site inspection. CBP then issues a written report, to be presented to the firm.[189] To date, less than 10% of C-TPAT certified participants have undergone and passed the validation process, achieving Tier II status.[190]

C-TPAT Security Criteria and Standards

C-TPAT security criteria are mandated for the three principal supply-chain participants: importers, highway carriers, and ocean carriers. The guidelines were intended to provide security expectations for all participating C-TPAT entities, as well as to set an industry

standard that firms could expect from one another. C-TPAT makes efforts to accommodate differences between various types of firms, and the security guidelines are intended to be flexible enough to apply to each individual carrier. Ultimately, the C-TPAT validation process is designed to ensure that the carrier is complying with C-TPAT regulations appropriately. Industry-wide, each firm must focus on the following issues in order to effectively increase supply-chain security: business partners, physical access controls, personnel security, procedural security, security training and awareness, container security, physical security and information technology security.

Security guidelines for all carriers govern the fundamental areas listed above. Below are the general guidelines. Carrier-specific guidelines are listed under separate headings.

Business Partners

Each firm must have documentation that its business partners are C-TPAT certified. If the partners are not certified, the importer must have proof that the partners, nonetheless, meet C-TPAT security requirements.

Container Security

Containers are protected using a variety of methods. A high-security seal must be used to properly close all loaded containers destined for the U.S. All containers must pass inspections of the front wall, left side, right side, floor, ceiling/roof, inside/outside doors, and outside/undercarriage. Finally, containers must be kept in a secure place when loaded and unloaded in order to prevent tampering.

Physical Access Controls, Personnel Security, Procedural Security, Security Training and Awareness

Access to the firm's facilities must be carefully protected. All employees should be identified and given access only to those areas in which they work. Background checks are required for employees. Badges should be issued to all employees, visitors and vendors. Deliveries should be regulated with all vendors displaying proper identification and packages being screened before dissemination. Security training and awareness programs should be implemented in order to increase awareness of the possibility and feasibility of a terrorist attack. Employees should be made aware of firm-specific procedures to follow in the event of an incident.

Physical Security and Information Technology Security

A firm's physical location should be secured according to C-TPAT guidelines. Various aspects of the location are governed by C-TPAT guidelines including fencing, gates and gate houses, parking, building structure, locking device and key controls, lighting, alarm systems, and video surveillance cameras. Finally, the information technology that a firm uses must be protected. Therefore, passwords used must be changed periodically, and technology security trainings should be offered regularly. A system must be put into place that identifies tampering with or improper access to data files.

Importers

C-TPAT guidelines for importers were instated on March 1, 2005. The regulations governing importers do not differ greatly from the general requirements expected of all firms.[191]

Sea Carriers

C-TPAT guidelines for sea carriers were instated on March 1, 2006. Specific only to sea carriers, C-TPAT is to be used in conjunction with the previous security measures of ISPS and MTSA. A sea carrier must be in compliance with these two initiatives before being considered for C-TPAT. C-TPAT members may only incorporate ISPS vessels into their fleets, and may only utilize ISPS-approved terminals to load and unload cargo. Certain aspects of the validation process, such as the physical access controls and physical security, can be validated through either ISPS or MTSA security guidelines. Sea carriers must pay specific attention to the risk of stowaways and follow particular procedures. For cargo not governed by ISPS regulation, physical barriers must be constructed to prevent unauthorized access. [192]

Highway Carriers

C-TPAT guidelines for highway carriers were instated on March 16, 2006. Regulations specific to highway carriers, include the provision for conveyance (tractor or trailer) security. C-TPAT mandates that highway carriers check their conveyances for hidden compartments. This search should occur at the points of entry and exit from the truck yard as well as at the final checkpoint reached, before crossing the U.S. border. CBP should be notified if a hidden compartment is discovered. Special seals are required for less-than-truckload (LTL) carriers to prevent unauthorized access to the truck.[193]

Critical Reviews of the C-TPAT Program

GAO Critiques

The Government Accountability Office (GAO) has produced several publications critiquing the C-TPAT program. While this report is not intended to simply repeat GAO's concerns, it is important to mention a few. Among the GAO's repeated criticisms are that CBP has not concretely defined the benefits that C-TPAT members will receive, that some members have been granted benefits prior to completing the validation process (including on-site inspections), that the validation process itself is not comprehensive enough, and that CBP does not have the personnel necessary to complete the validations in a timely manner.[194]

Trade Journal Critiques

While GAO critiques concentrate on lapses in security, for the most part, independent criticisms raised by trade journals concentrate on the lack of specifically-defined benefits awarded to C-TPAT members.[195] Until these benefits are more clearly defined at every level of C-TPAT compliance, firms are hesitant to pay to improve security procedures.[196]

The trade journals have also voiced concerns about the delay in realizing benefits that have already been promised. The so-called "GreenLane," for example, is dependent upon the Automated Commercial Environment (ACE) and "smart containers," while full functionality of those technologies are still years away; nevertheless, firms are obligated to meet the security requirements established for the GreenLane, today.[197] Further, trade journals are raising concerns about the changing nature of promised benefits.[198] Finally, and perhaps most importantly, these journals reflect the belief that changes have been made without adequate private-sector consultation.[199]

Much like the GAO, however, trade journals have also raised security concerns. Several authors have expressed concern that CBP is sending a mixed message by naming security as its number one priority, while implementing C-TPAT as a voluntary program.[200] The journals have also commented on the lack of public/private drills or exercises.[201] Firms want to undertake these drills as a means to better understand lines of command and standard practices, should an event occur that disrupts the flow of trade. Lastly, trade journals have questioned some of the security requirements themselves. For example, in order to achieve the Tier III rating (with access to the GreenLane), firms would be required to ensure the security of their goods from point of origin to point of entry in the United States. Some of the smaller firms though, believe they lack the necessary power and leverage to obtain such levels of security from suppliers and manufacturers.[202]

While the numerous articles written on C-TPAT provide valuable information and critiques, it is imperative to remember that journalists, not CEO's or C-TPAT members, write them. In order to gather industry-specific points of view, from the very people and firms being directly affected, we designed a survey to capture the thoughts and suggestions of firms within the trade industry.

Survey Analysis

The survey was designed to identify the shipping industry's responses to and opinions on C-TPAT. Questions were developed that allowed the shipping industry an opportunity to comment, confidentially, on various aspects of C-TPAT. The questions were also designed to gain a sense of the types of firms participating in C-TPAT and the reasoning behind their decisions to do so. For a complete listing of the questions included in the survey, please see Appendix 3a.

The survey was reviewed by the National Industrial Transportation League's (NITL) Select Committee on Security and then was distributed to members via e-mail in February 2006, by Peter J. Gatti, Jr., NITL Executive Vice President.

Participating Firm Statistics

Forty-four firms responded to the survey. Nearly 80% of respondents were members of C-TPAT, with 23% participating in Tier I, 27% in Tier II, and 12% in Tier III (the remaining percentage chose not to identify their designation). Annual firm revenues ranged from $450,000 to $60 billion. Responding firms employed anywhere between 1 and 122,000 people. Almost half classified themselves as importers, and another 40% chose not to identify themselves with the categories of carrier, shipper, or importer.

Nearly 60% of respondents ship more frequently over the Canada border, compared to 37% who more frequently cross the Mexican border. Of the responding firms, 93% shipped by truck, 86% by ship, 84% by air, and 59% by rail. Almost 82% use a broker when interacting with Customs.

Firms were asked to identify the primary incentives that would (or did) convince them to participate in C-TPAT. Nearly 46%, regardless of whether or not they were already C-TPAT members, stated that the incentives would need to be more persuasive and 27% stated that the program would need to be mandatory. When asked what keeps firms from participating in C-TPAT, 25% stated that the security requirements are too costly, while 23% decided that the benefits were not persuasive enough.

Conversely, participants were asked to rank the disadvantages experienced by choosing *not* to participate in C-TPAT. Almost 28% answered that CBP would continue to increase the security requirements, indefinitely, for C-TPAT as their primary disadvantage for not participating in the initiative. An increased number of inspections on non-member cargo, chosen by 30% of respondents was the second-ranked disadvantage. Almost 23% chose negative industry opinion as their third-ranked disadvantage of not participating in C-TPAT.

Finally, participants were asked to agree or disagree with several statements regarding C-TPAT. The most noteworthy responses are presented here:

Facility Security

- Close to 43% feel their computer system is the most secure aspect of their facility;
- 48% believe that a security breach to their facility could be repaired fast enough to stop a large-scale disruption;
- 45% state that there are security measures firms would like to employ, but lack the resources; and
- 50% feel that their storage containers are the least secure aspect of their facility.

C-TPAT Implementation

- 34% agree that C-TPAT regulations and application processes are clearly outlined;

- 36% agree that C-TPAT representatives are knowledgeable about the program;

- 43% believe that C-TPAT makes the country safer;

- 45% agree that C-TPAT requirements address the most vulnerable aspect(s) in the firm's supply chain; and

- 75% agree that their cargo clears Customs faster since joining C-TPAT.

Miscellaneous

- 32% agree that the competitive disadvantages of not participating in C-TPAT are significant; and

- 42% disagree with the idea that one level of standards should apply to all firms.

One of the most valuable aspects of the survey is the firms' anecdotal comments. Respondents' comments centered around several important themes, specifically: resources provided to fund the program; increased knowledge and skill by C-TPAT enforcers and valuators; and flexibility of the program in order to fit all types of firms. The three comments listed below most accurately capture general sentiments about C-TPAT.

- "C-TPAT is the only program or process with the flexibility to accommodate [sic] continued trade and [sic] improve the overall security deterrence [sic] effort. Congress does not have the depth of understanding of the international supply chain to regulate this import process effectively and should aggressively educate themselves on the issues. Currently the U.S. Customs is the only part of DHS that 'gets it' - and even they have issues. Fund the Customs better for overseas screening - any cargo discovered after it gets to a U.S. port has already slipped through... screening needs to occur long before arrival at U.S. ports."

- "Yes, CBP has been very slow to implement the mechanisms necessary, the program has become very bureaucratic [sic] and the officers are very slow to respond to any requests for help from the trade community. The centralization process that has taken place at CPB has really become a major obstacle to the advancement of this program. Decisions can only be made at Headquarters in DC, which has made the whole process very inefficient [sic] and confusing. Validators are poorly trained and in many cases the validation process is poorly performed."

- "C-TPAT needs to have more rigid guidelines and become mandatory. It is a very good first step that needs to be expanded a hundred fold."[203]

Similar C-TPAT Survey from CBP and COAC Proposes New Benefits

In January 2006, in response to continuous complaints from different members of the trade community, CBP announced it was in the process of designing a survey to be distributed to all C-TPAT members. CBP's survey will concentrate on quantifying both costs members have incurred in becoming C-TPAT compliant, as well as benefits (direct and indirect) received by the firms as a result of their participation in the program. In turn, survey results will serve to help member firms and prospective member firms quantify their investments and returns in the C-TPAT program.[204] The data collection portion of the survey was scheduled to be completed by March 2006; yet, as of July 2006, no results have been released.

Just prior to CBP's survey announcement, a subcommittee and task force of DHS' private-sector Commercial Operations Advisory Committee (COAC) recommended that C-TPAT members receive 12 new benefits for achieving Tier III status in the program. COAC conceived of the additional benefits in response to industry concerns that the C-TPAT program still lacks "quantifiable performance measures by which companies can judge the effectiveness of the program." [205] As of March 2006, three of COAC's proposed new benefits had been approved.[206]

Proposed Legislation Affecting C-TPAT

The two pieces of current legislation that will directly impact the future of C-TPAT are the House of Representatives' SAFE Port Act and its Senate counterpart, the GreenLane Maritime Cargo Security Act.

The SAFE (Security and Accountability For Every) Port Act: H.R. 4954

H.R. 4954 was recently introduced by Dan Lungren (R-CA), Chairman of the House Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity Chairman and Jane Harman (D-CA), Ranking Member of the House Intelligence Committee. H.R. 4954 contains similar provisions to S. 2459, The GreenLane Maritime Cargo Security Act of 2005 (see below). The bill would require the eventual 100% radiation scanning of containers as part of a timeline developed by DHS. The bill calls for the creation of a Port Security Grant Program to provide risk-based funding. The Secretary of Homeland Security is also required to establish joint-operations centers at ports to bring together security personnel from all layers of government, as well as to define protocols for restarting trade, in the event of a disastrous and disruptive incident. Additionally, the bill calls for the expansion of the Container Security Initiative (CSI) and the strengthening of C-TPAT through the creation of a top tier and the expansion of the validation process. Lastly, H.R. 4954 differs from S. 2459 in that it calls for the government to check all port employees' names against terrorist watch lists.[207] The bill which passed overwhelmingly in the House in May 2006 has been placed on the Senate Legislative Calendar under General Orders (Calendar No. 432) and is awaiting a Senate vote.[208]

The GreenLane Maritime Cargo Security Act (S. 2459)

Introduced on March 26, 2006 by Senator Susan Collins (R-ME), Chairwoman of the Homeland Security and Governmental Affairs Committee, and Senator Pat Murray (D-WA), S. 2459 calls for improvements in the CSI and C-TPAT programs, radiation scanning, the establishment of joint-operations centers, and the development of a strategic plan in case of disaster. The act is more explicit about the creation of, and requirements for, a GreenLane. [209] S. 2459, a re-introduced version of S. 2008, will be the basis for any legislative action in the remainder of the 109th Congress. The last Congressional action was taken on May 5, 2006, when it was placed on the Senate Legislative Calendar under General Orders (Calendar No. 424).[210]

U.S. vs. International Security Initiatives

Several other private-sector and public/private security initiatives are occurring concurrently with C-TPAT. Those detailed in the following section are viewed as most relevant and/or potentially relevant to C-TPAT.

Global Movement Management: IBM

IBM's Global Movement Management Initiative (GMM), is a framework presented as an answer to the largely piecemeal initiatives that are currently operating within the trade community. GMM offers both a "governance structure and a system architecture." According to the initiative overview:

> Global Movement Management is an integrated framework that looks holistically at the key variables in the system-flows, locations, modes of transport and exchange, and time – and finds areas of convergence across the existing system that are building blocks for enhancing security. These include: (a) common security and business functions, (b) existing borders and checkpoints, (c) existing data sources and information flows, and (d) existing relationships among key system participants.[211]

Rather than representing a set of laws and requirements that each firm must follow, Global Movement Management is a framework through which to view "security in a global economic system."[212] It emphasizes both security (protecting the system from attack) and resilience (minimizing potential effects of a disruption in service).[213] The building blocks of this framework are the commonalities existing in the global economic system, including:

- Common security and resilience-related business functions;
- Common control points, including national borders, movement chokepoints, and physical infrastructure;
- Existing data sources, transactions, and information flows that can provide inputs into the system; and

- Relationships among key system stakeholders.[214]

Authorised Economic Operator (AEO): European Union

The Authorised Economic Operator is the European Union's answer to C-TPAT. AEO was designed to provide certified traders with enforced trade facilitation measures.[215] AEO concerns itself with both the security of the supply chain, and other aspects of each individual firm, such as financial standing. Similar to C-TPAT, AEO tries to build upon existing security standards for maritime, air cargo and inter-modal shipping and does not intend to duplicate already functioning regulations. Like C-TPAT, AEO security guidelines are designed to be flexible enough to apply to large firms as well as medium- and small-size firms. Various supply-chain participants are held accountable for different criteria. Potential applicants can include manufacturers, exporters, forwarders, warehouse keepers, customs agents, carriers and importers.[216]

AEO's goal is to develop a framework that can be applied in all EU member states so that an AEO status given in one EU country will be accepted in another. A firm's application for AEO certification will need to satisfy three requirements, including:

- Compliance with Customs requirements;
- Successful management of commercial and transport records; and
- Proven financial solvency.

The benefits of AEO would include peer recognition of AEO status, reduced inspections, relaxed standards for pre-arrival and pre-departure requirements, and simplified procedures for Customs declarations. The anticipated results of the initiative include more reliable information, more clearly defined responsibilities, adopted data requirements, improved risk management, and improved control over exports. Most importantly, AEO strives to increase supply-chain security and to facilitate trade.[217]

Unlike C-TPAT, AEO allows applicants a choice in certification options. A firm may apply to either a Customs simplification option or a security facilitation option. Those complying only with Customs simplification must adhere to financial and Customs reliability requirements. If a firm wishes to qualify for the benefits received from security facilitations, the firm must comply with requirements for both the Customs simplification benefits and the security facilitation benefits. This allows for flexibility as a firm may apply for those benefits that directly benefit it. [218]

Lessons Learned and Conclusions

There is strong evidence that the United States remains at great risk for a terrorist attack on the maritime sector due to weak links in the supply chain and at ports of entry. Trade industry recommendations for the revision of C-TPAT are varied and often contradictory.

Some believe that C-TPAT should be mandatory, while others support its voluntary nature (see criticisms section above). Certain industry members believe that C-TPAT should become a cooperative effort between many government agencies, and not just a unilateral initiative of CBP. Some go so far as to say that the private sector should be much more engaged in port security discussion and even in policy development efforts.

However varied the suggestions for improvement, most industry respondents to the survey we administered believe that C-TPAT is not operating in the most efficient manner possible; they agree that C-TPAT is an inadequately funded program requiring security measures that are costly and, at times, even cost-prohibitive. Critics comment that C-TPAT should be flexible enough to work for firms of any size and that best practices should be publicly available and updated regularly. The lack of training for C-TPAT validators and the lack of consistent, reliable information regarding the program's requirements impede the successful implementation of a nation-wide security system and certainly stymie any attempt at a global security plan.

Critical to the success of C-TPAT are the benefits offered for to program participants. C-TPAT critics state that the benefits of program participation are too few, and those that are offered, at times, do not even exist. Many participating firms mention that aside from their certification status, direct benefits of being C-TPAT members, are non-existent.

U.S. firms acknowledge that C-TPAT is virtually useless if foreign participation is absent. Some members support the idea of including foreign firms in discussions about the future of C-TPAT in order to create a collaborative, international security effort. Also mentioned is the difficulty C-TPAT enforcers have in monitoring domestic ports and it is suggested that with a global effort, each country could provide and train its own C-TPAT staff.

On the whole, firms from all parts of the supply chain acknowledge and support the need for an industry-wide security initiative. Attention is being given to supply-chain security both due to recent realizations of U.S. vulnerabilities and as a result of industry-wide pressure to join C-TPAT. However, the pressure to join does not necessarily outweigh the perceived lack of advantages to participating in the program or the costs a firm must bear in order to be validated by C-TPAT. Much work remains to be done to include the opinions and suggestions of private-sector participants in future planning stages of C-TPAT, as well as to create avenues through which the international maritime supply-chain community can participate as well.

Appendix 3a
C-TPAT Survey

General Questions

1: Are you a member of C-TPAT?

Please choose only one of the following:

◊ Yes
◊ No

2: What tier are you participating in?

Please choose all that apply:

◊ Tier 1
◊ Tier 2
◊ Tier 3
◊ Not applicable

3: What is the size of your firm (annual sales)?

Please write your answer here:

4: What year was your company established?

Please write your answer here:

5: How many employees does your firm employ?

Please write your answer here:

6: Does your firm cross the U.S. / Mexico border or the U.S. / Canada border more frequently?

Please choose all that apply:

◊ U.S. / Mexico
◊ U.S. / Canada
◊ N/A

7: What methods of transportation do you use to move your goods?

Please choose all that apply and provide a comment:

◊ Air
◊ Truck
◊ Rail
◊ Ship
◊ Other
◊ No answer

8: Please specify your type of firm.

Please choose all that apply and provide a comment:

◊ Carrier
◊ Shipper
◊ Importer
◊ Other
◊ No Answer

9: If you interact with Customs, do you handle your Customs transactions in-house, or do you hire a broker to handle this aspect of your business?

Please choose all that apply and provide a comment:

◊ In-house
◊ Broker
◊ Other

10: What would convince you to participate in C-TPAT (1 being the most convincing benefit)?

Please number each box in order of preference from 1 to 7

◊ benefits more persuasive
◊ sufficient pressure from industry to join
◊ the program is mandatory
◊ security requirements less costly to implement

◊ security requirements less complex
◊ eligibility to participate in C-TPAT
◊ other, please explain on next page

11: Please rank the following barriers that prevent you from joining C-TPAT (1 being the largest barrier):

Please number each box in order of preference from 1 to 7

◊ benefits not persuasive
◊ insufficient pressure from industry to join
◊ the program is voluntary
◊ security requirements too costly to implement
◊ security requirements too complex
◊ not eligible to participate in C-TPAT
◊ other (please explain)

12: Please select the answer that is most appropriate, given the prompt

Please choose the appropriate response for each item:

Strongly Disagree Disagree Neutral Agree Strongly Agree Not Applicable

◊ C-TPAT representatives are knowledgeable enough about their program.
◊ C-TPAT regulations and application process are clearly outlined.
◊ Private companies instead of Customs should become involved in validating importers' supply chains in foreign countries.
◊ The premise of C-TPAT (preventing a terrorist attack) is realistic.
◊ There is a better way than C-TPAT to achieve supply chain security.
◊ C-TPAT works.

14: Is there anything specific you feel Congress should know regarding any of the issues addressed in the above questions, or any other C-TPAT issue (use this space to describe the "other" advantage from the previous question)?

Please write your answer here:

Perceived Advantages and Disadvantages

1: Please select the answer that is most appropriate, given the prompt.

Please choose the appropriate response for each item:

Strongly Disagree Disagree Neutral Agree Strongly Agree Not Applicable

◊ Our cargo has undergone fewer inspections since joining C-TPAT.
◊ Our cargo clears Customs quicker since joining C-TPAT.
◊ The proposed "green lane" will result in substantial benefits to my company.
◊ The competitive disadvantages for not participating in C-TPAT are large.

2: Please rank the following disadvantages to your firm for not participating in C-TPAT (1 being the biggest disadvantage).

Please number each box in order of preference from 1 to 7

◊ No access to FAST or green lanes.
◊ Fewer chances to participate in large supply chains.
◊ Increased security vulnerability.
◊ Increased number of inspections on cargo.
◊ Negative industry opinion.
◊ GAO recommendations to transform CBP validations into independent audits would be welcomed by my company.
◊ CBP will continue to increase the security requirements for C-TPAT.

3: Please rank from 1 to 6 the top six benefits that you receive from C-TPAT.

Please number each box in order of preference from 1 to 7

◊ Access to FAST or green lanes.
◊ More opportunities to participate in large supply chains.
◊ Increased security.
◊ Fewer inspections on cargo.
◊ Positive industry opinion.
◊ Insurance for continuity of operations in the event of a terrorist attack.
◊ Other (Please explain in the space offered for the next question)

4: Is there anything specific you feel Congress should know regarding any of the issues addressed in the above questions, or any other C-TPAT issue? (Use this space to describe the "other" advantage from the previous question)

Please write your answer here:

Security Questions

1: Please select the answer that is most appropriate, given the prompt.

Please choose the appropriate response for each item:

Strongly Disagree Disagree Neutral Agree Strongly Agree Not Applicable

- ◊ A security breach to my facility could be repaired fast enough to stop a large-scale disruption to the supply chain.
- ◊ My already-existing security system must be reconfigured in order to comply with C-TPAT regulations.
- ◊ The validation process is too rigorous.
- ◊ All firms, regardless of size, should have the same security requirements.
- ◊ C-TPAT makes the country safer.
- ◊ One level of standards and benefits should apply for all C-TPAT members.
- ◊ There are security measures that I would like to employ but lack the financial resources to do so.
- ◊ C-TPAT requirements address the most vulnerable aspect in my supply chain.

2: Please rank what you feel are the most secure aspects of your facility (1 being the most secure):

Please number each box in order of preference from 1 to 4

- ◊ Personnel
- ◊ Cargo containers
- ◊ Storage facilities
- ◊ Computer system

3: Is there anything specific you feel Congress should know regarding any of the issues addressed in the above questions, or any other C-TPAT issue?

Please write your answer here:

Submit Your Survey.

Chapter 4. The Framework of Standards to Secure and Facilitate Global Trade (SAFE)*

Introduction

In June 2005, member countries of the World Customs Organization (WCO) unanimously adopted the SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE). The voluntary agreement currently has 138 participating member countries and country-specific diagnostic missions, which constitute the first step in implementation, began in the fall of 2005.

SAFE compiles best practices for Customs administration security and trade facilitation, and sets an agenda for business participation, authorization, and inter-country Customs communication. The first section of this chapter provides the history and an overview of the WCO and a discussion of its key responsibilities. The next section outlines the key components of and provides a commentary on SAFE, followed by a description of the Columbus Programme and diagnostic missions to implement SAFE. The final sections discuss the role of the WCO within the international community as well as its relationship with the U.S. Customs and Border Protection (CBP).

Background of the World Customs Organization

Headquartered in Brussels, Belgium, the WCO employs approximately 100 people including 60 Customs experts.[219] Michel Danet (France) is the presiding Secretary General. He is assisted by Deputy Secretary General Kunio Mikuriya (Japan).

The WCO is divided into the Directorate of Compliance and Facilitation, headed by Director Michael Schmitz (United States), and the Directorate of Tariff and Trade Affairs, headed by Chriticles Mwansa (Zambia).[220] In June 2005, the WCO membership elected a third Director to lead the Directorate of Capacity Building. Lars Karlsson (Sweden) took office in January 2006.[221]

The mission of the WCO is "to enhance the effectiveness and efficiency of Customs administrations"[222] worldwide. As such, the three primary responsibilities assumed by the WCO are:

- To promote Customs, set standards and to develop and disseminate tools in order to help harmonize Customs systems and procedures worldwide;

* The acronym SAFE stands for Security And Facilitation in a global Environment and is the short name for the WCO Framework of Standards to Secure and Facilitate Global Trade.

- To assist member countries in their efforts to be compliant with existing international requirements by encouraging and helping to facilitate cooperation between members and with other international organizations; and

- To promote and facilitate member communication, cooperation and develop capacity in order to ensure that member countries are able to 'meet the challenges of the modern business environment and adapt to changing circumstances' and to compile and share best practices and other managerial and operational improvements that might be useful in updating and refining Customs practices.[223]

Today, WCO membership consists of 169 countries divided into six geographical regions: the Americas and the Caribbean; Europe - which extends to the Chinese border; North Africa and Near and Middle East; East and Southern Africa; West and Central Africa; and Asia-Pacific - which includes countries from Iran to Southeast Asia. These 169 member countries account for nearly 99% of worldwide trade. Interestingly, approximately 80% of WCO membership could be categorized as developing or in transition to a market economy. [224] The 2005/2006 general funding budget of the WCO is approximately €12.6 million (US$16.1 million), slightly less than 25% of which is provided by the U.S.[225]

WCO Initiatives and Programs

In its nearly 60 years of existence, the WCO has worked to develop and help implement conventions and other international instruments through which it aims to harmonize international Customs procedures. The following are some of the programs and initiatives introduced by the World Customs Organization:

Harmonized Commodity Description and Coding System

This system entered into force in January 1988 and provides uniform 6-digit subheadings for traded goods. There are over 100 contracting parties to the Harmonized System Convention as well as additional participating countries. The Convention facilitates the harmonization and uniform application of a simplified and effective Customs system. The harmonized classification system is currently the common global standard for imports and exports.[226] The WCO acts as an arbitrator in harmonization disputes, and creates binding agreements between parties.[227] Partners include the World Trade Organization (WTO), United Nations (UN) Statistics Division and the UN Environmental Program.[228]

General Agreement on Tariffs and Trade (GATT) Customs Valuation Agreement

This agreement replaced the contested 1952 Convention on the Value of Goods for Customs Purposes (more commonly known as the Brussels Determination of Value). As the 1952 Convention had failed to gain widespread approval, the idea for GATT arose as a compromise during one of the multilateral trade negotiations. The GATT Valuation Code came into existence in 1981 and was replaced in 1994, renamed the WTO

Valuation Agreement. The agreement determines the value of goods for Customs duties and taxes with the WTO taking the leading role in the valuation process.[229]

1973 Kyoto Convention (and its 1999 revision)

Formerly known as the International Harmonization and Simplification of Customs, the Convention serves as an international instrument that facilitates the harmonization of Customs techniques in addition to covering all facets of Customs legislation. The Convention was revised and updated in 1999 as the exponential growth and development of both international trade itself and technology had left conventional Customs procedures outdated. Convention partners include the International Code Council and the International Express Carriers Conference.[230]

Customs Enforcement Network (CEN)

In 1983, the WCO established the Enforcement Committee to come up with viable strategies to combat Customs violations and offenses. One of the more recent initiatives of the Committee is the Customs Enforcement Network (CEN), which utilizes a modern electronic database "to facilitate cooperation in the field of enforcement and the dissemination of information and intelligence."[231] Compliance and enforcement partners include the UN Office on Drugs and Crime, World Intellectual Property Organization, WTO, UN Education, Scientific and Cultural Organization, International Centre for Migration Policy Development, European Commission (EC), Convention on International Trade in Endangered Species of Wild Flora and Fauna, International Atomic Energy Agency, and UN and private-sector, anti-smuggling programs.[232]

Training and Trade Facilitation

Finally, the WCO provides a number of training and technical cooperation opportunities for its members. These include informational meetings, promotion of recommended best practices, raising awareness, and training seminars. Training is conducted through expert missions, training courses, and workshops. The WCO also administers fellowship programs and increasingly distributes information through electronic medium.[233]

Customs Organizational Development

Since the mid-1990s, the WCO has developed a range of services to assist members in reform and modernization. By means of the diagnostic framework, the WCO provides strategic organizational development for Customs. Conducting in partnership with members an extensive diagnostic program, and providing action planning and business case development service. This is supported by a regionally-based network of capacity building centers.[234]

Although the above functions help to facilitate global trade at large, the WCO remains positioned as a leading intergovernmental organization focusing on the harmonization of Customs administrations and systems.[235]

Previous WCO Involvement in Security

The WCO has long been involved in international security efforts. In addition to the 2003

adoption of international conventions on information exchange in Nairobi and Johannesburg, South Africa, it is also responsible for the creation and implementation of the aforementioned Customs Enforcement Network (CEN), an electronic database containing information on narcotic, tobacco, intellectual property rights, and other seizures as well as offering guidelines on intelligence.[236] The WCO also engages in risk profiling and has implemented a harmonized risk management methodology.[237]

The SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE)

The WCO has received an unprecedented number of member country pledges to implement the SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE). The comparative success of this initiative to other WCO initiatives, given such wide-ranging international support, is enhanced by the WCO's commitment to work with each member country that commits to implementing the Framework. [238] Member country support for SAFE ranges from Sweden's significant monetary contribution in support of the Capacity Building component, to the U.S.' commitment to in-kind support, such as site assessments and training.[*]

While commitment to SAFE is voluntary, the general belief is that countries will be at a competitive disadvantage for international trade if they do not participate.[239] Joe Kelly, in the WCO's Capacity Building Directorate, believes that if SAFE were binding in nature, the number of countries willing to commit would be greatly reduced and implementation would take significantly longer due to member country ratification processes.[240]

History of the Development of SAFE

- **2002**: A Task Force on Security and Facilitation is proposed by former U.S. Customs and Border Protection (CBP) Commissioner, Robert Bonner. The group was formed and compiled a comprehensive list of work to be done.

- **December 2003**: The U.S. proposes the creation of a High Level Strategic Group (HLSG) to assume the responsibilities of the Task Force and to develop the SAFE Framework of Standards. Twelve member countries formed the HLSG.

- **June 2005:** WCO Council unanimously agrees to adopt SAFE and 90 member countries commit to implementation.

---

[*] The U.S. has not contributed financial aid in support of SAFE as U.S. Customs must be specifically authorized by Congress to do so. As the U.S. has not received Congressional authorization to contribute funds to SAFE, it is assisting through in-kind donations of time and training.

- **October 2005:** Florida meeting is hosted by CBP to craft implementing guidelines for the Framework.

- **December 2005:** Implementing guidelines are presented to WCO Policy Commission.

- **June 2005 - Present:** Secretary General Danet undertakes a worldwide promotional tour to raise awareness about and gain support from member countries for the Framework.

- **June 2005 – Present:** Customs administrations begin diagnostic missions.

- **June 2006:** 138 of the 169 WCO member countries have committed to implement the Framework.

Components of SAFE

The WCO cites two premises for the need to implement SAFE. First, as the facilitation of trade is the underlying driver for safer supply chains, "the world need[s] a strategy to prevent terrorism without jeopardizing the flow of trade."[241] Second, SAFE is intended to provide "uniformity and predictability in the trade environment and safeguard end-to-end security of the legitimate supply chain and facilitate the flow of legitimate goods."[242]

SAFE establishes standards for supply-chain security and facilitation, supply-chain management, enhancement of the capabilities of Customs administrations and strengthens networking amongst Customs administrations and in cooperation with the private sector. The majority of the standards are based on current WCO measures and member-developed programs.

Developed with four main goals in mind, SAFE aims to:

1. Harmonize information and data fields on advance electronic manifests;
2. Develop and implement a common approach for risk management;
3. Conduct examinations with non-intrusive detection equipment; and
4. Offer concrete benefits to private firms*.[243]

Given these goals, SAFE includes two pillars: the Customs-to-Customs Pillar and the Customs-to-Business Pillar.[244] In addition to the pillars, there is a capacity-building initiative, the Columbus Programme, to help implement the Framework.

* Firms that conduct self assessments of the security of their supply chains, which are then validated by the Customs administration, are then granted authorised economic operator (AEO) status which includes various benefits, such as faster clearance times.

Customs-to-Customs Pillar

SAFE's Customs-to-Customs component is designed to provide common, internationally accepted Customs standards in an attempt to encourage and facilitate cooperation and information-sharing among Customs administrations worldwide. Such critical communication and intelligence sharing will ensure maximization of security and facilitation at all levels of the international trade supply chain.

The Customs-to-Customs Pillar draws upon a number of practices that CBP has initiated since 2001 and resembles parts of the Container Security Initiative (CSI).[245] The main components of this Pillar include the use of advance electronic information on inbound, outbound and transit shipments; risk management; outbound inspection of high-risk consignments; smarter and more secure container technology; and employee integrity.[246]

The advance information component requires shippers to supply Customs authorities with an advance manifest prior to arrival at a foreign port.[247] The risk management component of the Framework highlights information sharing for Customs administrations by ensuring that inspections and other techniques will be used to screen containers and cargo.[248]

Industry concerns about the Customs-to-Customs Pillar have been raised both about the inclusion of an export focus for many Customs administrations, as well as about the number of data elements countries should be required to use for risk assessment.

Many developing countries still rely on Customs (import) revenue as their primary source of government funding.[249] The proposed shift to an export-focused (out-bound) system thus poses a challenge for such member countries. Even in some developed countries, the collection of Customs duties is substantial. "In the U.S., Customs duties amount to $18 billion[*] per year, while in the European Community they represent 15% of total revenues."[250] While revenue collection remains the current focus of developing countries, the European Union feels it is changing this paradigm by proposing that Customs can stay competitive when it can also guarantee the security of its exports.[251]

SAFE calls for the collection of 27 data elements[†] in order to conduct a risk analysis.[‡] The private sector has expressed concern regarding this list, asking how many data elements Customs administrations need to adequately conduct risk assessment of cargo.[252] CBP, for example, currently requires only 11 data elements[253] for its analysis, though an additional ten elements have been proposed and are under consideration for implementation.[254]

Robert Ireland, Technical Attaché to the WCO, believes that although the types of data elements were recommended as a means to facilitate the work of Customs administrations, most countries will not utilize the entire list the WCO has outlined.

---

[*] Unless otherwise noted, all currency is listed in U.S. dollars.

[†] For a complete listing of the 27 Customs data elements required by the WCO, refer to Appendix 4a.

[‡] For a complete list of the 27 data elements under the Customs microscope, please refer to Appendix 4b.

There will always be overlap in the types of elements collected, but at a minimum, Ireland recommends between 10 and 15, as fewer than 10 would not solicit a diverse indication of the risks. Unfortunately, according to Joe Kelly of the WCO, some data elements may always be contentious as they include the sensitive area of commercial value.* For a complete list of standards within the Customs-to-Customs Pillar, refer to Appendix 4b.

Customs-to-Business Pillar

SAFE's Customs-to-Business Pillar is similar to the U.S.' Customs-Trade Partnership Against Terrorism (C-TPAT) program.[255] The idea behind this pillar is that, in order to maximize efficiency and effectiveness in securing the international trade supply chain, Customs administrations must partner and collaborate with the private sector. Much like C-TPAT certification, this Pillar aims to develop a system for identifying firms whose supply chains meet and/or exceed supply-chain security standards. Such firms will be certified and receive benefits for their continued commitment to security. In June 2006, the WCO Council adopted an "Authorized Economic Operator"[256] (AEO) document, which is divided into a core standards section and a national standards section. One delegation has further proposed a new section "N" to the document, which would add a provision on automation and technology. Among other things, this additional section would provide for secure AEO computer network. This proposed section will be up for discussion and consideration for adoption, in December 2006.

As it currently stands, the AEO document "provides baseline technical guidance for the implementation of AEO Programmes at the global level between WCO Members and the international trade community."[257] The document serves as a starting point for the national Authorized Economic Operator Programme implementation and supports the effective application of the standards that are outlined in the Customs-to-Business Pillar of the SAFE Framework. "This guidance will provide for long-term application of meaningful standards that will apply to both Customs and Authorized Economic Operators at the global level. These *core international standards* shall form a baseline that must be followed by all parties engaged in this effort. This document also allows for the inclusion of *supplemental national criteria* that may be required by any given Customs administration."[258]

As noted in the previous chapter, the European Commission is working on its own Authorised Economic Operator (AEO) program, a similar initiative for European Union member countries, designed to be compatible with the WCO's program for future global trade.

---

* The accurate valuation of goods creates tensions between developed and developing worlds because the former wants to pay as few customs duties as possible, while the latter wants to collect as many as possible. Post-clearance audits are used by auditors to see that the appropriate duty was accounted for during a customs transaction. The formal customs clearance doesn't occur until the post-clearance audit has been certified. This is the only point at which the real invoice must correlate with the invoice that came through customs. The attraction of the developing world to the Framework is to get more accurate valuation data into the global trading system.

In order to enhance and improve upon this process, the WCO has created a Private Sector Consultative Group (PSCG). The PSCG provides the WCO with industry recommendations for security and trade facilitation. PSCG members serve one-year terms with the option to serve a second term. Members are chosen based on the geographic relevance of the issues. An expected 30th member of the current PSCG will be from Africa. The PSCG meets in Brussels two to three times, per year.[259] For a complete list of PSCG members, refer to Appendix 4c.

In the spring of 2006, the WCO formed the Mercury Club, a forum for the entire private sector to express concerns and recommendations on issues of Customs modernization and reform.[260] Private-sector members are also invited to attend WCO training sessions to educate their internal clearance and Customs staff on new procedures.[261]

Recently, firms have voiced concerns that small and medium enterprises (SME) in the Customs-to-Business Pillar may not have the financial capability to secure their supply chains, putting them at a trade disadvantage.[262] The WCO believes that not enough research has been done to determine the benefits for SMEs. One problem is that it is difficult to find an international organization to represent SMEs in WCO consultations because they tend to be country specific. Research is being commissioned by the WCO this spring to further examine the issue.[263] For a complete list of standards within the Customs-to-Business Pillar, refer to Appendix 4d.

Columbus Programme

The Columbus Programme is SAFE's capacity-building initiative. Its goal is to promote the adoption and implementation of SAFE while building sustainable, long-term capabilities for Customs administrations.[264]

Capacity building will be implemented at the member-country level. Under the supervision of its Director General responsible for Customs, each country will conduct a self-assessment. A team of WCO trained facilitators* will then conduct a strategic diagnosis at which point the country will appoint an implementation manager to oversee the process and act on the diagnostic recommendations. The implementation manager will report on progress until completion of the process. Finally, the WCO will conduct a review of the completion of implementation.[265]

Some trade journals have expressed concern that the WCO is not a mature enough international organization to be working on such an expansive and long-term initiative. They argue that other organizations, such as the International Maritime Organization (IMO), have a legacy of international agreements that are binding on their members. Additional challenges include funding for the capacity-building initiative, and government-level complications within member countries.

Fundraising

*As of July 2006, 80 Facilitators have been accredited to conduct WCO Diagnostic Missions.

To date, the U.S., EU, Japan, Canada, Sweden, UK, Russia, the Netherlands, France, South Africa, Italy, India and Australia have pledged to support the Columbus Programme.[266] The U.S., EU, Norway, the Netherlands, Russia, Australia and Canada will provide in-kind support for the program, ranging from site assessments and providing diagnostic missions to capacity building and training. Sweden, the UK, South Africa, Italy and India have all provided the WCO with financial support. Each member country is designated as a no-cost, low-cost or high-cost country, according to cost estimates of implementation.[267] An estimated $15 to $20 million will be devoted to training customs personnel in advance electronic collection of shipping manifests, risk analysis and the use of x-ray equipment.[268] Additional technology items will be dependent on funding from international financial organizations such as the World Bank, Inter-American Development Bank, US Agency for International Development, and the Organization of American States. Currently, both China[269] and Russia have received loans from the World Bank for Customs modernization. Russia has received $146 million.[270] For comparison, New Zealand expects to spend $15 million to implement its diagnostic recommendations.[271]

Government Level Complications

In November, 2005, the *Journal of Commerce* reported findings from a survey conducted by the IBM Institute for Business Value Survey. The survey focused on countries working on "modernization and standardization of cross-border activities."[272] The key barrier identified by businesses operating in member countries was that the legal and political actions of member-country governments were interfering with fluid, efficient operations.[273]

According to Robert Ireland, the U.S. recognizes that implementation of the Framework will be a long process, and that some member countries may never fully achieve its standards. It is believed, however, that most countries that have committed to implementation will have begun the process in the very near future.[274]

Cross-departmental management and communication, legislative change, training, and integrity represent some of the more commonly identified problems within Customs administrations. The challenge facing implementation of the Framework will be for member countries to incorporate changes in their national legislation to give Customs administrations more authority to oversee export-related activities.[275] Moving away from a traditionally import-focused Customs regime will be difficult in and of itself, but the actual legislative processes required by member countries in order to realize this shift will render the task all the more difficult and time consuming. "The specific legislation in most countries that needs the most work is data exchange and the power to give information to another organization, particularly one outside of the country."[276] For many countries, current laws make data exchange difficult as regulatory information is often embedded within the code. A specific job description for example, may be part of the Customs code. The WCO will work with member countries to encourage information-sharing policies and will provide model legislation as a guideline.[277]

Employee training and integrity are human resource issues for Customs administrations. While SAFE's immediate goal is to provide participating countries with the technological capacity needed for implementation, its larger goal is to develop and maintain a workforce that is thoroughly trained and willing to utilize the technology and resources available. Though most member countries, for example, already have some kind of computerized Customs system, it is unclear who is responsible for and/or sufficiently trained to troubleshoot technological problems as they arise. On the other hand, having a constant stream of trained officers, with additional technical support, may be a difficult human resource management issue for Customs administrations.[278]

Working to ensure employee integrity in Customs administrations will be the next step. "Someone has to manage the technology to see that it is actually being used, and not deliberately broken so officials can go back the old system"[279] of corruption and bribery. In some countries, the existence of illegal activity may be so entrenched in Customs practices that it is thought to be a part of legal Customs procedures. As an example, Kelly recalls an officer's salary scale explanation: "Every car that comes across the border we charge $10, every truck we charge $30. At the end of the week, the shift leader divides the money [according to rank of the officer]." There was no legal basis for collecting these fees, but this kind of practice was not uncommon. The truck driver may have even believed that this was the legal fee.[280]

With regard to employee integrity in Customs administrations the WCO's goal is to educate Customs officers and private-sector participants about what constitutes a criminal act and potential repercussions of being involved in such an act.

Pilot Projects and Diagnostic Missions

The WCO anticipates conducting over 50 diagnostic missions to member countries over the next 18 months. In addition, developed member countries such as the United States, Canada, Scandinavian countries, Japan, Australia and New Zealand will conduct approximately 40 of their own site assessments and trainings.[281] The United States, for example, will conduct site assessments for 11 countries; the UK, France, the Netherlands and Russia will provide experts for diagnostic missions; and the EU will be working on a provisional list of developing EU countries with which to conduct diagnoses and capacity building.[282] While some of the more developed member countries that have committed to SAFE (such as the U.S.) do not need capacity building, for those that do, all diagnostic work will be concluded by June 2007.[283]

The diagnostic framework to be utilized by the WCO is largely based on the Revised Kyoto Convention of 1999. The Convention addresses seven components of the Customs organization, including strategic management; human resources and logistics; legislation, procedures; use of technology; external relationships; and integrity and governance. The U.S. will use a separate, but complementary diagnostic tool.[284]

The WCO has also begun (and successfully completed 17) diagnostic facilitator training workshops to certify both public and private participants. Previous private-sector participants have included Crown Agent, Emerging Markets, Price Waterhouse Coopers,

Cotecna, and Greenline Systems. Approximately 20-25% of training participants will be certified to use the diagnostic framework, with an ultimate goal of 80 certified facilitators to be available worldwide.[285]

As of July 2006, the WCO has successfully conducted 17 diagnostic missions to Guatemala, Madagascar, Ethiopia, Cambodia, Lesotho, Moldova, China, Cameroon, Mongolia, Bahrain, Panama, Rwanda, Bermuda, Serbia and Montenegro, Brazil, South Africa, and Vietnam. Joe Kelly is confident that these countries will be assisted in acquiring the necessary funding to move forward with their implementations. In addition, the WCO regions of Asia-Pacific and East and Southern Africa will be starting their own capacity-building programs within the year.

International Partnerships

Upon taking office on January 1, 2006, one of the first actions of the Director of Capacity Building was to meet with international organizations to promote ties and establish joint missions and seminars to enhance SAFE's implementation. Some international organizations have their own Customs programs, so the WCO is working to increase the areas where those programs overlap with SAFE. The partnerships that were highlighted in the history section above are not included in this section.

International Organization for Standardization (ISO)

In November 2005, the ISO published the first in a series of supply-chain security recommendations, ISO 28000, and 28001. ISO 28001 is seen as the more controversial of the two, because as it offers more specific details about applying security measures. A subcommittee of the ISO is currently working on ISO 28004, a companion document whose goal is to help companies understand and implement the security standards.

In September 2005, ISO representatives met with WCO representatives, giving the WCO an opportunity to evaluate the standards to ensure they aligned with those outlined in SAFE. In response, the WCO submitted suggestions and held a subsequent meeting with ISO members in the spring of 2006.

U.S. Support for and CBP Involvement in SAFE

The first major post-9/11 programs implemented by CBP were C-TPAT and CSI. They were first put forth to prioritize U.S. security and to enhance benefits for large U.S. traders. The WCO hopes to use SAFE as a means to spread these initiatives worldwide, providing equal access for all parties.[286]

The U.S. has its own capacity building initiative, which is run through CBP's International Affairs office, headed by Assistant Commissioner E. Keith Thomson. The U.S. is currently conducting site assessments of 11 countries. U.S. support will be awarded based on the country's commitment to implementing SAFE. A second selection criterion for U.S. support will be a diverse geographic representation. Some countries already selected by the U.S., include the Dominican Republic, Ghana and South Africa.[287]

CBP Programs and the WCO Framework

SAFE draws upon several key elements of the U.S. programs initiated by former CBP Commissioner Robert Bonner in the wake of September 11, 2001. As SAFE modifies initiatives such as CSI and C-TPAT, several potential problems exist with respect to the U.S. agreeing to the new terms. First, the Framework calls for both import and export security standards. Currently, through CBP, the U.S. only employs the import portion of SAFE.[288] One potential barrier to implementing the export portion is that U.S. Census regulations prohibit sharing any information collected by the Automated Export System (AES) of a shipper's export declaration, with foreign governments.[289] Second, there are interagency aspects of Customs that need to be more clearly defined, such as CBP interactions with the U.S. Commerce Department.[290]

Lessons Learned and Conclusions

The World Customs Organization's SAFE Framework of Standards to Secure and Facilitate Global Trade is an important step towards modernization and reform for many Customs administrations. While the current push from the United States is aimed at strengthening security, the goals and benefits of such an initiative for Customs modernization in other countries may be more diverse.

SAFE is a long-term commitment to Customs modernization and strategic planning. In spite of pledged funding, diagnostic missions and private-sector support, systemic change in many Customs administrations may come slowly due to a lack of political will within member countries.

While the aggregate number of member countries that have committed to SAFE has exceeded expectations, each will enter the implementation stage at a different level of interest and capability. For developed member countries, the focus is on security, from terrorism to counterfeit goods and intellectual property rights, because these are viewed as a real threat and the country's ability to cope with this threat is also significant. SAFE will also play a role as an enhancement mechanism for compliance and enforcement.[291]

A majority of member countries will coalesce around trade facilitation because they realize that inefficient Customs administrations can block economic development in their countries if they aren't sensitive about their relationship with the global trade network.

SAFE will enable the WCO to challenge member countries to define and/or redefine their respective Customs administrations to reflect individual country and political values. The security piece of SAFE will enable all Customs administrators to enhance plans in the event of a catastrophic natural event, which could undermine global trade for the country.[292]

As a large percentage of member country governments rely on the duties collected by their Customs administrations, the proposed modernization will foster a more efficient, comprehensive collection system.

Additional issues will need to be resolved to ensure that all member countries and private-sector participants are ultimately on a "level playing field." At the forefront of such issues are the mutual recognition of all member country Authorised Economic Operators, the inclusion of small and medium enterprises in WCO decision-making and the supply-chain security network, and the legislative compromises that governments and government agencies must make to implement the Framework.

The World Customs Organization has a successful history of working with international organizations including the World Trade Organization and the United Nations, and is working to expand its network through increased publicity, and personal interactions with political, business and organizational leadership. Looking towards the future, additional players, such as health ministries and immigration agencies, will need to be added to the mix to enhance new security issues associated with global trade.

Appendix 4a
27 Data Elements

1.) Consignor/exporter
2.) Description of goods
3.) United Nations dangerous goods code if applicable
4.) Type of packages
5.) Number of packages
6.) Unit of measurement
7.) Total gross weight
8.) Total invoice amount
9.) Currency
10.) Place of loading
11.) Carrier
12.) Equipment/unit load device number
13.) Equipment size/type
14.) Seal number
15.) Identification of the means of transport (license plate number of truck, Lloyd's number of ship, tail number of aircraft)
16.) Name of the country of the means of transport
17.) Carrier-defined conveyance reference number
18.) Methods of payment of transport charges
19.) Customs office of exit
20.) Country or countries of routing
21.) First port of arrival
22.) Date and time of arrival at first port
23.) Consignee/importer
24.) Notify party
25.) Delivery destination
26.) Agent
27.) New "unique consignment reference"

From: Philip Damas, "Global Security Controls on Supply Chains," *American Shipper*, August 2003, p. 24.

Appendix 4b

Customs-to-Customs Pillar Standards
World Customs Organization
Framework of Standards to Secure and Facilitate Global Trade, June 2005

Standard 1 – Integrated Supply-Chain Management

The Customs administration should follow integrated Customs control procedures as outlined in the WCO Customs Guidelines on Integrated Supply Chain Management (ISCM Guidelines).

Standard 2 – Cargo Inspection Authority

The Customs administration should have the authority to inspect cargo originating, exiting, transiting (including remaining on board), or being transshipped through a country.

Standard 3 – Modern Technology in Inspection Equipment

Non-intrusive inspection (NII) equipment and radiation detection equipment should be available and used for conducting inspections, where available and in accordance with risk assessment. This equipment is necessary to inspect high-risk containers or cargo quickly, without disrupting the flow of legitimate trade.

Standard 4 – Risk-Management Systems

The Customs administration should establish a risk-management system to identify potentially high-risk shipments and automate that system. The system should include a mechanism for validating threat assessments and targeting decisions and identifying best practices.

Standard 5 – High-Risk Cargo or Container

High-risk cargo and container shipments are those for which there is inadequate information to deem shipments as low-risk, that tactical intelligence indicates as high-risk, or that a risk-scoring assessment methodology based on security-related data elements identifies the shipment as high-risk.

Standard 6 – Advance Electronic Information

The Customs administration should require advance electronic information on cargo and container shipments in time for adequate risk assessment to take place.

Standard 7 – Targeting and Communication

Customs administrations should provide for joint targeting and screening, the use of standardized sets of targeting criteria, and compatible communication and/or

information exchange mechanisms; these elements will assist in the future development of a system of mutual recognition of controls.

Standard 8 – Performance Measures

The Customs administration should maintain statistical reports that contain performance measures including, but not limited to, the number of shipments reviewed, the subset of high-risk shipments, examinations of high-risk shipments conducted, examinations of high-risk shipments by NII technology, examinations of high-risk shipments by NII and physical means, examinations of high-risk shipments by physical means only, Customs clearance times and positive and negative results. Those reports should be consolidated by the WCO.

Standard 9 – Security Assessments

The Customs administration should work with other competent authorities to conduct security assessments involving the movement of goods in the international supply chain and to commit to resolving identified gaps expeditiously.

Standard 10 – Employee Integrity

The Customs administration and other competent authorities should be encouraged to require programs to prevent lapses in employee integrity and to identify and combat breaches in integrity.

Standard 11 – Outbound Security Inspections

The Customs administration should conduct outbound security inspection of high-risk containers and cargo at the reasonable request of the importing country.

Appendix 4c

WCO Private Sector Consultative Group Membership

American Association of Exporters and Importers
Boeing
BP
Business Alliance for Secure Commerce
Carrefour
China Ocean Shipping Co.
FedEx
General Motors
Global Express Association
Hutchinson Port Holdings
IBM
International Air Transportation Association
International Alliance of Ports and Harbors
International Chamber of Commerce
International Chamber of Shipping
International Federation of Customs Brokers Associations
International Road Transport Union
Japan Machinery Center for Trade and Investment
Limited Brands
Maersk Sealand
Microsoft
Moscow International Business Association
Nissan
Phillips International
Procter & Gamble
Siemens
SITPRO
Thales
World Shipping Council

From: Chris Gillis and Eric Kulisch, "Going Global with Security," *American Shipper*, January 2006, p.38.

Appendix 4d

Customs-to-Business Pillar Standards
World Customs Organization
Framework of Standards to Secure and Facilitate Global Trade, June 2005

Standard 1 – Partnership

Authorized Economic Operators involved in the international trade supply chain will engage in a self-assessment process measured against pre-determined security standards and best practices to ensure that their internal policies and procedures provide adequate safeguards against the compromise of their shipments and containers until they are released from Customs control at destination.

Standard 2 – Security

Authorized Economic Operators will incorporate pre-determined security best practices into their existing business practices.

Standard 3 – Authorization

The Customs administration, together with representatives from the trade community, will design validation processes or quality accreditation procedures that offer incentives to businesses through their status as Authorized Economic Operators.

Standard 4 – Technology

All parties will maintain cargo and container integrity by facilitating the use of modern technology.

Standard 5 – Communication

The Customs administration will regularly update Customs-Business partnership programs to promote minimum security standards and supply chain security best practices.

Standard 6 – Facilitation

The Customs administration will work co-operatively with Authorized Economic Operators to maximize security and facilitation of the international trade supply chain originating in or moving through its Customs territory.

Chapter 5. Brazil and the Port of Santos

Introduction

Brazil is the largest country in South America. With a total geographic area of more than 8.5 million sq km, Brazil is only slightly smaller than the United States of America. Its estimated 2006 population is 188,078,227. In 2005, Brazil's estimated Gross Domestic Product reached US$619.7 billion*, growing at an annual real rate of 2.4%. Brazil's leading economic sectors are services, 50.6%; industry, 39.4%; and agriculture, 10%. Key industries include textiles, shoes, chemicals, cement, lumber, iron ore, tin, steel, aircraft, motor vehicles, auto parts and machinery.[293] With its enormous geographic span, Brazil has over 7,491 km of coastline, 29,412 km of railways, 50,000 km of waterways, and 1,724,929 km of highways (94,871 km paved).[294]

Brazilian global exports amounted to $118.3 billion in 2005 ($65 billion manufactured, $35 billion basic, and $16 billion semi-manufactured). In the same year, the country saw a 22.6% increase in exports[295]. The U.S. is the leading purchaser of Brazilian goods, accounting for 19.2 %, or $22.7 billion, of exports in 2005. Leading export sectors include transportation material, metallurgical products, soybeans, oil and fuel, ores, meats, chemicals, machinery and equipments, electrical equipment, sugar, leather, footwear and apparel, and paper and pulp.[296] More than 80% of Brazil's foreign trade is concentrated at the following ten ports (port, state):

- Itajaí, Santa Catarina;
- Itaqui, Maranhão;
- Paranaguá, Paraná;
- Rio de Janeiro, Rio de Janeiro;
- Rio Grande, Rio Grande do Sul;
- Santarém, Pará;
- Santos, São Paulo;
- Sepetiba (now Iguatai), Rio de Janeiro;
- Vila do Conde, Pará; and
- Vitória, Espírito Santo.

Appendices 5a and 5b delineate the top ten Brazilian export destinations, as well as principal ports of departure.

---

* Unless otherwise noted, all currency is listed in U.S. dollars.

National Structures

Port Administration/Authority

CONPORTOS

Port security is the responsibility of the National Commission for Public Security in Ports, Port Terminals, and Navigable Waterways *(Comissão Nacional de Segurança Pública em Portos, Terminais e Vias Navegáveis, CONPORTOS)*. CONPORTOS is the primary body responsible for port security in Brazil. The commission, established on May 30, 1995 by Decree 1507, and altered by Decree 1972 on July 30, 1996, predates passage of ISPS. CONPORTOS is an inter-ministerial body presided over by the Ministry of Justice that comprises members from the Ministries of Justice, Finance, Transportation, Defense, and Foreign Relations.

The objectives of CONPORTOS are to "elaborate and implement the system for preventing and repressing illegal acts at ports, terminals, and navigable waterways." CONPORTOS is tasked with the following responsibilities:

- Create the State Commissions for Public Security in Ports, Port Terminals, and Navigable Waterways *(Comissões Estaduais de Segurança Pública em Portos, Terminais e Vias Navegáveis, CESPORTOS)*;
- Interact with international financial institutions for technical and financial assistance;
- Advise on legislation (improvements);
- Analyze public security programs at ports, terminals and navigable waterways;
- Maintain a statistical database of illegal incidents at ports, terminals and navigable waterways;
- Monitor the results of investigations into illegal incidents and the remedies/punishments applied;
- Orient CESPORTOS; and
- Analyze and approve risk assessments and security plans created by CESPORTOS.[297]

CONPORTOS comprises several entities tasked with responsibilities for port administration and security:

> **Federal Police** *(Departamento de Polícia Federal-DPF)* - DPF is responsible for inspecting ships suspected of crimes, including acts of terrorism and/or illicit acts linked to weapons trafficking (conventional, biological, chemical and nuclear).[298]

DPF has established Special Maritime Police Groups (*Núcleos Especiais de Policia Maritima-NEPOM)* to police port areas via land and water. Seven NEPOMs have been organized specifically to combat drug trafficking at Rio Grande (*Rio Grande do Sul*), Itajaí (*Santa Catarina*), Paranguá (*Paraná*), Vitória (*Espírito Santo*), Foz do Iguaçu (*Paraná*), Recife (*Pernambuco*) and Belém (*Pará*).[299]

Brazilian Navy *(Marinha do Brasil)* - The Navy is responsible for assuring waterborne security and safety along Brazilian coast and inland waterways.[300]

Federal Revenue Secretariat *(Secretaria de Receita Federal-SRF)* - The SRF is part of the Brazilian Ministry of Finance and serves as Brazil's Customs organization. The SRF is responsible for inspection of cargo involved in foreign trade and for maintaining Customs control of imports and exports at ports and inland dry ports. The Port Law of 1993 (*Lei dos Portos*, No. 8.630, Dec. 25, 1993) is the chief law that granted SRF its legal jurisdiction.[301] SRF's role in administering security measures ultimately falls under the responsibility of its Coordinator General (*Coordenador Geral de Administração Aduaneira, COANA*).

Port Authorities – Local Port Authorities are responsible for internal policing of ports, conducted by the Port Police (*Guarda Portuária*); for regulation of the entry and exit of persons, cargoes and vehicles; and for policing of port facilities, installations, cargo and equipment (protection of patrimony).[302]

Other entities serve limited roles in port security, including the Civil Police, Military Police and the Fire Department.

Ministry of Trade

Presided over by the Ministry of Trade, the Foreign Trade Council (*Camara de Comercio Exterior, CAMEX*) is an official organ that monitors foreign trade activities. Among CAMEX's attributes is the orientation of Customs practices. CAMEX is responsible for monitoring C-TPAT, CSI, ISPS, and the U.S. Bioterrorism Act, as well as measures emanating from ALADI and Mercosul. CAMEX is composed of:

- The Minister of Development, Industry and Commerce (Trade Ministry);
- Presidential Chief of Staff;
- The Minister of Foreign Relations;
- The Minister of Finance;
- The Minister of Agriculture;
- The Minister of Health; and

- The Minister of Planning.[303]

CAMEX is organized into an executive committee, financial committee and a private-sector consultative committee made up of 20 representatives from diverse segments of the private sector.[304]

Ministry of Transportation

Through Ministry of Transportation Directive No. 495 of December 16, 2004, the Ministry of Transportation established priorities for a national policy of port infrastructure. Subsequently, Directive GM No. 33.2005 of February 24, 2005 created the Permanent Working Group for Ports (*Grupo de Trabalho Permanente, GTP-Portos*). The GTP is tasked with monitoring the emergency activities and priority actions of national port policy. The Department of Waterborne Transport Programs' National Director, Paulo de Tarso Carneiro, coordinates the GTP. The GTP has four sub-groups related to different ports. The groupings are:

- Santos, Salvador, Aratu;
- Itajaí, São Francisco do Sul, Paranaguá;
- Rio de Janeiro and Itaquí; and
- Sepetiba and Vitória.

When solicited, the designated port authorities are charged with submitting operational performance data to the GTP on a weekly basis.

PROHAGE

Created by Inter-ministerial Directive No. 11, on November 25, 1997, the National Commission for Harmonization of Activities of Agents of Authorities in Ports (*Comissão Nacional de Harmonização das Atividades dos Agentes de Autoridades nos Portos - PROHAGE*) works to integrate port activities and optimize any actions related to the dispatch of ships, cargo, crew, and passengers.

Port Funding

Funding to implement Brazilian port security measures comes from several sources. Provisional Measure 184 (*MP 184*) of May 2004 dedicated R$100 million for port security and infrastructure. Allocation of these funds was split between several different ministries: the Ministry of Transportation - R$57.3 million, the Ministry of Justice - R$39.5 million and the Ministry of Defense (Navy) - R$3.2 million. Moreover, Provisional Measure 161 (*MP 161*) of Jan. 21, 2004 earmarked 25%of the funds from the national gas tax (*CIDE*) to be used for port infrastructure. Appendix 5c notes the ten ports, as federal port authorities, that received programmed resources in 2005 for ISPS implementation.

CONPORTOS and CESPORTOS are currently lobbying the Brazilian government to pass legislation that would create a National Fund for Public Port Security (*Fundo Nacional de Segurança Pública Portuária*). It should be noted that Brazil's macroeconomic policy of inflation targeting and its generation of a primary surplus has hindered investment programs across all sectors, as authorized funds are withheld until certain targets are met. This has disrupted port funding and, more generally, transportation as a whole.

In other funding areas, the government passed port modernization legislation (*Regime Tributário para Incentivo à Modernização e à Ampliação da Estrutura Portuária - REPORTO*) that exempted several taxes levied on the importation of port equipment, such as post-panamax cranes, rubber-tire mobile cranes, reach-stackers, forklifts, weighing machines, and portainers. The exemptions save approximately 30-40% of the purchase costs for the equipment. As a result, many terminals at Itajai, Santos and Paranaguá have significantly upgraded their facilities. Appendix 5c delineates federal resources allotted to port authorities in 2005. The REPORTO legislation will remain active until the end of 2007.[305]

Port Case Study - Santos

General Port Information

The Port of Santos is South America's largest port and the largest container port in Latin America. The port is managed by the Santos Port Authority (*Companhia das Docas do Estado de São Paulo, CODESP*), a state-owned entity linked to the Ministry of Transportation. With more than 54 terminals, Santos lies just 100 km from the city of São Paulo, Brazil's most populous city and home to its greatest concentration of industry. The port handles a diverse mix of commodities, led by sugar, coffee, citrus, soybeans, soy meal, wheat, salt, fertilizers, petroleum and petrochemicals, and machinery and vehicles. Santos hosts 61 berths; twelve berths are dedicated to container ships and four multi-use berths can also handle containers.[306] The Port of Santos occupies a ship channel with a total length of 11,600 meters and an area of 7.8 million sq meters. Port berths have depths ranging from 6.6 to 13.5 meters.[307] There are 45 warehouses in the internal area of the port (34 on the right bank and 11 on the left bank); additionally, there are 39 warehouse facilities near the internal port area.[308]

In 2005, the Port of Santos was responsible for 26.5 % of Brazil's commercial trade (exports and imports). Of the 5,535 vessels arriving in Santos in 2005, 4,385 were involved in international trade.[309] Santos was responsible for $32.8 billion of Brazil's $118.3 billion export cargoes in 2005.[310] Appendix 5d presents Santos' cargo movements both in tons and TEUs. As a load center for international cargo, Santos bears a strategic role in trade with the United States. The United States is Santos' largest export destination, accounting for $5.8 billion, or 17.7%, of total Santos exports in 2005.[311]

ISPS at the Port of Santos

National Implementation

Implementation of ISPS (*Codigo Internacional de Segurança e Proteção de Embarcações e Instalações Portuárias*) is the responsibility of CONPORTOS. As elaborated earlier in this chapter, CONPORTOS comprises an inter-ministerial group, led by the Ministry of Justice and its National Secretariat for Public Security (*Secretaria Nacional de Segurança Pública, SENASP*), and authorized by the IMO to implement, accompany, and monitor ISPS. CONPORTOS has subordinated the responsibilities for collecting information, and developing and submitting risk assessments, security plans, and certification requests to the State Commissions, CESPORTOS. CESPORTOS also receives the certification applications of port security organizations. Only certified port security organizations can participate in the development of port security plans for ports, terminals and related facilities.[312]

Every port and port terminal is required to create its own risk assessment, delineating threats and security weaknesses, and a security plan. These risk assessments and security plans are approved by CESPORTOS and filed with the Regional Superintendencies of the Federal Police. If deemed necessary, CESPORTOS has the authority to appoint a Coordinator for Port Security, who would then become responsible for inspection, maintenance and execution of plans related to ISPS implementation at the port in question. Such a job would likely fall to the Coordinator of CESPORTOS or an official within the Port Authority.[313]

Following approval and certification from CESPORTOS, the final approval of port risk assessments, security plans, inspection and certifications of compliance falls to CONPORTOS. Once a security plan is approved, within a year of the initial submission of a risk assessment, a first inspection is undertaken. This inspection is conducted by teams of six inspectors, three from CONPORTOS and three from CESPORTOS. The ports and port terminals are required to have follow-up certifications every five years, with inspections to occur no less than 3 years apart.[314]

CONPORTOS organized the Brazilian port structure into the following groups by state:

- Group 1: Santa Catarina, Paraná, Mato Grosso do Sul, and Rio Grande do Sul;
- Group 2: Alagoás, Sergipe, Piauí, and Bahia;
- Group 3: Rio de Janeiro, Espírito Santo, Pernambuco, and Amapá;
- Group 4: São Paulo, Paraíba, Rio Grande do Norte, Ceará; and,
- Group 5: Maranhão, Amazonas, Roraima, Pará, and Mato Grosso.[315]

In order to facilitate compliance with ISPS, a special designation was created, called the Term of Aptitude (*Termo de Aptidão - TA*). The TA is issued to a port or port facility if its security plan has been approved, but not yet fully implemented.

As of March 20, 2006, CONPORTOS had approved 218 security plans. Security plans are submitted both by the ports and terminals. For a port to receive the Declaration of Compliance (*Declaração de Cumprimento - DC*), each of its facilities must have obtained its own individual DC. Of the 218 facilities (terminals and ports) with approved security plans, 127 have been granted DCs. Seventy-five installations are still in the implementation phase (Term of Aptitude) and sixteen facilities have not yet been inspected, indicating that 91 port facilities are still not fully compliant with ISPS.[316] Appendix 5e lists the status of ISPS implementation at each Brazilian port.

Local Implementation

As per CONPORTOS Resolution 5 of June 27, 2004, port security plans are the responsibility of the port authorities and must be submitted to CESPORTOS-SP and the Federal Police. CESPORTOS for the State of São Paulo (*CESPORTOS-SP*) is responsible for the Port of Santos.

The Santos Port Authority (*CODESP*) contracted with the University of São Paulo to create the first elements of a port security plan (*Sistema de Segurança Pública Portuária, SSPP*). Santos' final risk assessment and security plan were approved in 2004. Funding for the first phase of the plan's implementation, in the amount of R$13.98 million, was provided through Provisional Measure 184 of May 10, 2004. At the end of 2005, R$10.12 million of the total R$13.98 million had been allocated. Brazilian government regulations require ports to hold a public bidding process for any acquisitions of equipment, construction, or facility improvements related to ISPS implementation. Following this process, the Port of Santos signed its first contracts in July 2004 and the main installations of new facilities and equipment were completed by August 2005.

Although ISPS implementation has been a priority for the Brazilian government and CODESP, and allocated funding has been directed for such purposes, the financial situation at the Port of Santos is less than optimal. The port is on the brink of being unable to pay its renegotiated debt service through the federal program Refis (*Refinanciamento de Dívidas Federais*). At present, CODESP has a debt of approximately R$700 million (more than US$300 million).[317] Of this debt, R$400 million constitutes back taxes owed to the federal government. The remaining debt is the result of labor disputes. Terminal operators are also in poor financial situations. Two major port terminal operators, Libra Terminals and the São Paulo Steel Company (*Companhia Siderurgica Paulista, COSIPA*) are in arrears to CODESP. According to CODESP, as of June 2006, Libra owes nearly R$400 million and COSIPA owes R$250 million.[318]

Adding to the dire financial situation at the port, the federal government's practice of inflation targeting has led it to freeze budgetary authorizations. Authorized funds are held by the Treasury contingent on primary surplus performance. This fund freeze has affected all government ministries, agencies, and programs including CODESP. In 2005, CODESP received approval for R$101.3 million in funding. At year end, merely R$13.8 million, or 13.6%,of this amount had been spent. The financial situation at the

port is worth noting because it has greatly affected CODESP's ability to implement port projects. Implementation of ISPS is one of the few port programs to be executed, while other port projects such as dredging and landside access have been significantly delayed.[319]

Santos Port Security Plan (Sistema de Segurança Pública Portuária - SSPP)

On September 19, 2005, CODESP and the University of São Paulo released the first phase of the Santos Port Security Plan (*SSPP*), which delineated a process for restricting vehicular and human access to Santos' 28 access gates and 54 terminals.[320] Access to gates and facilities is limited by turnstiles; in addition, cameras, hand keys, walls, and fences are also central to the SSPP. By the end of 2005, 228 cameras had been installed. Appendix 5g describes the restriction of access gates at Santos.

The SSPP also requires the creation and use of personal identification cards for all persons that will access ships, terminals and port facilities. The plan established an on-line registration system to expedite registration and documentation for diverse port participants, such as truckers and companies located far from Santos.[*] Identification cards contain an individual's photo and biometric data obtained via palm print. Some problems surfaced in the early development of these ID cards, as many workers complained about having identical family names. Thus, after initially requiring both first and last names to be listed on the ID card, it was decided to only include a worker's photo and first name.[321] Santos began distribution of its identification cards in September 2005. The identification badges are coded to grant access to specific facilities based on job function and responsibility. Appendix 5f specifies the access permissions by title and function.

Credentialing

Santos is now implementing ISPS access procedures, issuing identification badges and carrying out biometric screening. Screening is carried out on two levels: 1) controlled access (within port, but no access to ships), and 2) restricted access (access to ships). Controlled access procedures use badges, while restricted access procedures will use both badges and biometric data (hand keys).[322] In April 2006, Santos announced a new hybrid security effort that would use badges to screen persons and vehicles, while manually checking those individuals who had not yet gone through the credentialing process.[323] By June 2006, Santos had begun applying this system of access, permitting manual checking of identification by the Municipal Guard in addition to checking badges. This system will likely become permanent, as it facilitates easier identification checks on individuals, such as out-of-state truckers, who do not yet possess the new identification badges.[324]

A major effort has been made to register port workers and those needing access to the port. CODESP is responsible for all credentialing procedures and printing of

[*] The website where individuals and companies can register for port access is http://www.ispssantos.com.br.

identification cards. In order to facilitate the registration of workers, CODESP called on the port's private companies, as well as trade and labor unions, to gather information on their personnel. The following organizations were among those called upon to register their workers:

- Casual Workers Management Organ (*Orgão Gestor de Mão de Obra OGMO*);
- Port Operators Sindicate of the State of São Paulo (*Sindicato dos Operadores Portuários do Estado de São Paulo, SOPESP*);
- Maritime Navigation Agencies' Sindicate of the State of São Paulo (*Sindicato das Agencias de Navegação Maritima do Estado de São Paulo, SINDIMAR*); and
- Truckers Sindicate (*Sindicato dos Caminhoneiros, SINDICAM*).[325]

As a direct result of credentialing port workers for photo and biometric identification, casual port worker rolls dropped from 9,000 to approximately 7,500. The number of casual port workers with job functions and registrations at a specific port terminal also dropped, temporarily leaving the entire roll of casual port workers at 6,250. By May 5, 2006, more than 17,000 persons and vehicles had been registered. It is expected that this number will increase to an eventual total of 25,000 registered persons and vehicles. In addition to the categories listed above, there are provisions in place for granting temporary access to visitors, crew, and eventually, transport service providers.

Criticism of these new security measures, including ISPS, has been focused on the costs of implementation. Many terminals and businesses claim they cannot afford the necessary equipment. Container terminal operators have admitted that they are passing the costs of implementation onto port users through higher rates. For example, Sergio Salomão, President of the Brazilian Association of Public Use Container Terminals (*Associação Brasileira dos Terminais de Conteineres de Uso Públic - ABRATEC*), stated in September 2005 that six out of ten private container terminals were already raising their rates to cover costs. According to Salomão, rates were being raised by an average of R$31 per TEU, which represents an increase of 0.07% of the TEUs value.[326]

ISPS Compliance by Port Terminals

Before Santos can achieve full ISPS compliance, each of its terminals must have received its individual declaration of compliance (DC). The Working Group within the Office of Institutional Security of the President of the Republic and CONPORTOS set a deadline of June 30, 2006 for full compliance of all ports (and terminals).

ISPS Next Steps

The Port of Santos is working to complete the next stages of ISPS implementation through the development of a three-level alert system. As designed, the system comprises the following levels: 1) no threat, normal; 2) danger; and 3) invasive event (terrorist attack). The system, to be fully defined by the end of 2006, would link ship-to-

shore communications.

CSI

On May 24, 2005, Secretary of the Federal Revenue Secretariat, Jorge Antônio Deher Rachid, signed a declaration of principles with the United States for the Port of Santos to participate in the Container Security Initiative (CSI).[327] On September 26, 2005, the initiative was launched and Santos became the first port in South America, and the 39th port in the world, to join the program. Per the Customs exchange component of CSI, U.S. Customs and Border Protection maintains a presence at the Port of Santos to inspect and monitor containerized cargo bound for the United States. As per the reciprocal nature of the exchange, Brazilian Customs has the opportunity to place inspectors on U.S. soil to inspect and monitor containerized cargo bound for Brazil. The first port contemplated for such purposes is the Port of Miami, Florida.

As a part of the CSI program, the U.S. government donated an x-ray machine to scan containers. Though the x-ray machine was delivered to the Libra Group's Terminal 37, it is mobile and circulates to the other container terminals of note, namely Rodrimar, Tecondi, and Santos Brasil. To be fully effective, the CSI program will require three mobile scanners, two for the right bank (Libra, Tecondi, Rodrimar) and one for the left bank (Santos Brasil-Tecon).

Other U.S. Participation

The U.S. Coast Guard and CONPORTOS conducted a joint evaluation of Brazilian ports in September 2005. Participants visited the Ports of Santos, Fortaleza/Mucuripe, Pecém, Rio de Janeiro, and Sepetiba to evaluate the implementation of new security measures.[328]

On June 20, 2002, the United States also signed a Customs Mutual Assistance Agreement with Brazil. This agreement is based on bilateral cooperation models used by the World Customs Organization. However, the agreement is not yet in force.[329]

Lessons Learned and Conclusions

The modern structure for Brazilian port security predates the events of September 11, 2001. The establishment of CONPORTOS/CESPORTOS in 1996 created the necessary institutional structure to articulate and execute port security programs and planning. However, the events of 9/11 were a catalyst to spur these entities to greater action. In addition, ISPS, CSI and multiple other international security programs have accelerated Brazil's implementation of new security policies. Such programs have been largely responsible for the modernization of Brazil's ports.

Unfortunately, although Brazil has agreed to adopt international security standards, implementation of these standards has been proceeding at a slow pace. As of March 2006, 218 Brazilian ports and port facilities were participating in international trade. Of these ports, 97 have not yet received a Declaration of Compliance for ISPS. Even

Santos, the nation's largest port, had not achieved full compliance as of May 2006. Implementation of ISPS has been conditioned on Brazilian budgetary restrictions, inflation targeting and public bidding procedures. In order to facilitate the compliance process, Brazil created a Term of Aptitude to identify ports and facilities that are making progress but awaiting their final Declaration of Compliance from CONPORTOS. Of the 97 ports and facilities that are not yet compliant, nineteen had yet to see their first CONPORTOS inspection by the end of March 2006.

The Brazilian federal government is aware of the slow pace of compliance at Brazilian ports. In an effort to speed up the process, the Office of Institutional Security of the President of the Republic reactivated an inter-ministerial Working Group for the purpose of pressuring ports to achieve compliance. The working group comprises 14 members from the Ministries of Justice, Defense, Transportation, Planning, Trade, as well as the President's Chief of Staff (*Chefe da Casa Civil*). Those ports not yet in compliance with ISPS are now threatened with fines unless they complete the necessary steps to gain compliance. The ports in worst condition are Rio de Janeiro and Itaguai. Exemplary ports having received ISPS certification are Itajai, Fortaleza, São Francisco do Sul, Suape and Pecém.

At the Port of Santos, implementation of ISPS has brought about some unexpected, indirect benefits, possibly leading to permanent efficiency gains. As a result of the credentialing component of ISPS implementation, it has become far more difficult for stevedores to continue the practice of allowing others to work in their place. However, anecdotal evidence that implementation costs have been passed from CODESP on to individual terminal operators suggests that the competitive advantage of increased efficiency may be eliminated by increased operations costs.

The difficulties caused by the poor financial situation at the Port of Santos and the limits this may place on future advances in port security cannot be underestimated. The federal government's economic policy of inflation targeting and freezing authorized funds impedes progress towards effective and efficient port administration and, as a result, ISPS implementation. ISPS implementation was funded under exceptional circumstances, a special Provisional Measure issued by the Executive branch of the federal government. Without significant own-source funding, the frequent delays from waiting on federal funding seem likely to continue.

In spite of Brazil's adoption of ISPS and CSI, most Brazilian officials see these programs as an added cost. In Brazil, there is little concern about the direct threat of terrorism. However, those interviewed also see the benefits of modernizing port security. They agree that ISPS has been responsible for bringing about system-wide improvements that have generated momentum for other port projects. In this sense, ISPS has helped a backward port sector advance towards becoming competitive in the international arena.

Appendix 5a

Brazilian Export Destinations 2005 (U.S.$ FOB)

Rank	Country	Value (U.S.$ FOB Billions)	Share (%)
1	United States	22.7	19.2
2	Argentina	9.9	8.4
3	China	6.8	5.8
4	Holland	5.3	4.5
5	Germany	5.0	4.2
6	Mexico	4.1	3.4
7	Chile	3.6	3.1
8	Japan	3.5	2.9
9	Italy	3.2	2.7
10	Russia	2.9	2.5

Source: *Brazilian Trade Balance-Consolidated Data*, Ministry of Development, Industry and Foreign Trade, Brasília, DF, 2006.

Appendix 5b

2004 Exports of Merchandise from Brazilian Ports (U.S.$ FOB Billions)

Rank	Port	State	Value (U.S.$ FOB Billions)	Share (%)	% Change 2004/2003
1	Santos	SP	26.89	27.88	33.03
2	Vitória	ES	8.72	9.04	24.99
3	Paranaguá	PR	7.96	8.26	23.35
4	Rio Grande	RS	6.90	7.15	20.80
5	Rio de Janeiro	RJ	3.85	3.99	15.13
6	Itajaí	SC	3.74	3.87	25.97
7	Sepetiba	RJ	3.59	3.72	66.40
8	São Luis (Itaqui)	MA	2.83	2.93	69.72
9	São Francisco do Sul	SC	2.81	2.91	26.31
10	Salvador	BA	2.26	2.34	24.02
11	Munguba	PA	1.35	1.40	41.35
12	Macaé	RJ	1.20	1.25	100.31
13	Aratu	BA	1.07	1.11	20.97
14	Manaus	AM	0.85	0.88	33.84
15	Niterói	RJ	0.80	0.82	6,005.27
16	Pecém	CE	0.73	0.76	102.69
17	São Sebastião	SP	0.71	0.74	-17.32

Source: Ministry of Development, Industry and Foreign Trade, Secex, Brasília, 2005.

Note: Excluded from this table but included in the calculations of share are exports from airports and border crossings.

Appendix 5c

Programmed Resources for Federal Port Authorities in 2005

Port	**State**	**Authorization**
Aratu	Bahia	R$500 thousand
Belém	Pará	R$1 million
Fortaleza	Ceará	R$500 thousand
Ilheús	Bahia	R$500 thousand
Salvador	Bahia	R$500 thousand
Santarém	Pará	R$500 thousand
Santos	São Paulo	R$9.5 million
Sepetiba	Rio de Janeiro	R$2 million
Vila do Conde	Pará	R$500 thousand
Vitória	Espírito Santo	R$2 million

Source: CONPORTOS.

Appendix 5d

Port of Santos Cargo Movement

Year	Tons (millions)	TEUs
2000		946,064
2001	48.2	1,047,695
2002	53.5	1,224,354
2003	60.1	1,560,201
2004	67.6	1,882,639
2005	71.9	2,267,921

Source: Port of Santos Annual Report 2005, pp. 6-8.

Appendix 5e

ISPS Code Implementation Status by Port to March 20, 2006

Port (State)	ISPS Compliant	Port (State)	ISPS Compliant
Antonina (Paraná)	No	Porto Alegre (Rio Grande do Sul)	No
Aratu (Bahia)	No	Porto da Ilha (Rio Grande do Norte)	6/2/2005
Belém (Pará)	No	Recife (Pernambuco)	No
Cabedelo (Paraíba)	No	Rio de Janeiro (Rio de Janeiro)	No
Fortaleza/Mucuripe (Ceará)	7/8/2004	Rio Grande (Rio Grande do Sul)	No
Ilhéus (Bahia)	No	Salvador (Bahia)	No
Imbituba (Santa Catarina)	No	Santarém (Pará)	1/26/2006
Itajaí (Santa Catarina)	7/8/2004	Santos (São Paulo)	No
Itaqui (Maranhão)	3/23/2005	São Francisco do Sul (Santa Catarina)	2/4/2005
Macapá	1/28/2005	São Sebastião (São Paulo)	No
Maceió (Alagoás)	No	Sepetiba (Rio de Janeiro)	No
Manaus (Amazonas)	No	Sepetiba CVRD (Rio de Janeiro)	7/8/2004
Miramar (Pará)	No	Sotave (Pará)	No
Natal (Rio Grande do Norte)	6/2/2005	Suape (Pernambuco)	8/11/2004
Paranaguá (Paraná)	No	Vila do Conde (Pará)	No
Pecém (Ceará)	7/12/2004	Vila Velha (Espirito Santo)	No
		Vitória (Espírito Santo)	No

Source: Ministry of Justice, CONPORTOS, Instalações Portuárias-Quadro Geral, March 20, 2006, accessed May 4, 2006 http://www.mj.gov.br/senasp/conportos/.

Appendix 5f

ID Card Specifications

Type	Function	Priority	Code
Customs Workers	Persons and vehicles assigned with responsibilities to Customs	1	10
Workers from Other Authorities	Persons and vehicles from other authorities, Federal Police, Civil Police, Ministry of Agriculture, Ministry of Labor, etc.	2	14
Directors of CODESP	Members of the Board of Directors of CODESP and vehicles	3	11
CODESP Employees	Employees and vehicles of CODESP	4	5
Customs Service Providers	Persons and vehicles serving Customs, contractors etc.	5	4
CODESP Service Providers	Persons and vehicles serving CODESP	6	2
Union Workers	Persons and vehicles representing port-related trade unions	7	13
Service Providers for Port	Persons and vehicles representing companies that perform services for the port, such as maritime agents, port operators	8	3
Pilots	Persons and vehicles that carry out piloting services for the port	9	9
Drivers	Persons and vehicles that represent transport providers, cooperatives and independent autonomous trucker	10	15
Press	Persons and vehicles representing the press (newspaper, radio, television)	11	12
OGMO Workers	Persons and vehicles with management link to the OGMO	12	6
Casual Workers	Casual port workers (stevedores, longshoremen, tallymen, etc.)	13	16

Source: Fundação de Apoio à Universidade de São Paulo (FUSP), Sistema de Segurança Pública Portuária-Fase I: Cartilha de Controle de Acesso nas Áreas Restritas do Porto de Santos , São Paulo, SP, September 19, 2005.

Appendix 5g

Port of Santos' Access Gates

Gate	Location	Gate	Location
1	Petrobrás Administration at Alemoá	15	CBA-TEAG Pier
2	Alemoá Access	16	Terminal Libra 35
3	Piers of Alemoá	17	TEAG Pier
4	Deicmar and Saboó Pier	18	Terminal Libra 37
5	Rodrimar	19	Macuco
6	Piers at Warehouses 10/11	20	Export Corridor
7	Pier at DIROP	21	Quayside Libra 37
8	VCP	22	ADM
9	Teaçu	23	Entry to the Presidency of CODESP
10	Copersucar	24	Exit at Presidency of CODESP
11	Concais	25	Exit/Entry of Officials at area of CODESP Administration
12	T-Grão	26	Landside access to Barnabé Island
13	Canal 4	27	Piers at Barnabé Island
14	Citrosuco/NST	28	Oceanside Access to Barnabé Island

Source: FUSP, SSPP, pp. 15-16.

Chapter 6. France and the Port of Marseille

Introduction

France is the largest Western European state. With a total land area of 547,030 sq km, it is slightly less than twice the size of the state of Colorado. In 2005, the population of France was estimated at 60,656,178 and its Gross Domestic Product was estimated to be US$2.118 trillion*, consisting of: agriculture, 2.5%; industry, 21.4%; and services, 76.1%. In 2005, France's exports amounted to $443.4 billion, of which 6.7% were destined for the United States; its imports totaled $473.3 billion, of which 5.1% originated in the U.S. France boasts 29,519 km of railways, 891,290 km of highways, 8,500 km of waterways and 3,427 km of coastline. Major ports and inland terminals include Bordeaux, Calais, Dunkerque, La Pallice, Le Havre, Marseille, Nantes, Paris, Rouen, and Strasbourg[330].

National Structures

Port Administration

France is the world's 5th largest exporter and the 6th largest importer of goods (in nominal dollars). It is responsible for 12% of the total exports of the European Union (EU), over half of which are transported by sea. The French Ministry of Transportation, which oversees all maritime activity, identifies three categories of maritime ports: Autonomous Ports (*Ports Autonomes*), Ports of National Interest (*Ports d'Intérêt National*) and Decentralized Ports (*Ports Décentralisés*).[331]

Autonomous Ports

All major French ports, with the exception of The Port of Calais (*Port de Calais*), operate as autonomous ports in accordance with 1965 law. Book I, Title I of the *Seaports Code* defines an autonomous seaport as a port that is charged with the:

- development, improvement and maintenance of port infrastructures;
- general management, police and upkeep of port docks and premises;
- general management, police, safety and security of movements of ships and goods; and
- management and industrial-commercial development of large public land assets.[332]

There are currently eight Autonomous Ports in France, accounting for 76% of the total national freight traffic. These ports operate under federal control. Each of the seven

* Unless otherwise noted, all currency is listed in U.S. dollars.

major metropolitan ports (Marseille, Le Havre, La Rochelle, Dunkerque, Rouen, Nantes-St-Nazaire and Bordeaux) handles between nine and seventy-six million tons of cargo annually; the eighth, an island port off the coast of France, Guadeloupe, handles an annual average of two million tons. Autonomous Ports are directly administered by private boards composed of 25 members each, and a Chief Executive Officer (generally a highly ranked civil servant), appointed by the Council of Ministers. Most employees in Autonomous Ports, with the exception of the most senior port officials, who are generally appointed by the state, operate as private laborers under French employment law.[333] These private laborers are either hired by shipping, handling and/or freight forwarding companies contracting with the Port Authority (as are most dockworkers), or by staffing agencies (as are many of the security officers.)[334]

As public initiatives, Autonomous Ports are subject to the state's financial control; however, in some instances, they are permitted to purchase shares in other public or private companies, thereby engaging in and promoting economic partnerships.[335]

According to the Maritime Ports Code, the main priorities and investments of each Autonomous Port are defined by the federal government, and differ from port to port. Operations, maintenance and policing of the ports are entrusted to the Port Authorities themselves, and are not often overseen by the state.[336]

Ports of National Interest

The second group of seaports in France, accounting for 22% of the total national freight traffic, is the Ports of National Interest. These twenty, largely commercially active seaports are organized under the legal provisions set forth in Book I, Title II of the *Seaports Code*, and will remain under state control until 2007. They include sixteen metropolitan ports (Calais, Boulogne-sur-Mer, Dieppe, Caen-Ouistreham, Cherbourg, Saint-Malo, Brest, Le Fret, Roscanvel, Concarneau, Lorient, Bayonne, Port-la-Nouvelle, Sète, Toulon, and Nice) as well as the four overseas ports of Martinique, Guyane, Saint-Pierre and Miquelon, and Reunion. Management responsibilities for the Ports of National Interest are shared by the local branch of the Ministry of Transport[*] and the local Chamber of Commerce.[†]

France is currently in the midst of a significant transition with respect to port management and ownership. In July 1983, Law N° 83-663[337] initiated a shift from state to more local and regional control of ports and other elements of maritime infrastructure. Upon the adoption of this legislation, fifty commercially active seaports came under local control. These fifty decentralized ports, currently account for 2% of the total national tonnage. In accordance with Law N° 2004-809[338], the control of most of the remaining Ports of National Interest will be transferred to the local and/or regional (depending on the nature of the port's primary commercial activities) governing

[*] Responsible for building/maintenance, oversight of port police, and for monitoring accounts of port commercial operator

[†] Acts as public commercial operator, oversees facilities, land-based equipment and superstructures

authorities by January 1, 2007.[*] The decentralization of French ports (which includes major roads, airports and most Ports of National Interest) is an effort both to relieve some of the strain on the state's budget and to enhance the local and regional economies in France. The eight Autonomous Ports are expected to retain both their legal public status and federal funding and are not currently being considered for decentralization[339].

Decentralized Ports

The final category of French seaports is Decentralized Ports. These are the smallest and least commercially significant of the French seaports. There are a total of 532 Decentralized Ports, of which 304 are fishing and commercial ports, managed by the Ministry of Transports' regional officials and 228 are tourism and sailing ports, managed by local authorities.[340]

France's Autonomous Ports are the only ports of significance for the purpose and scope of this report; as such, these are the only ports that will be examined in further detail.

Customs Regime

Organization/Hierarchy

The French Customs and Excise Service – CES (*La Douane*) reports to the Minister of Finance, Economy and Industry. Its staff of 20,000 (split between its Paris headquarters and its "Outfield" offices[†]) is overseen by a Commissioner, nominated by the Prime Minister and appointed by the President. The Commissioner is assisted by a Private Cabinet, Internal Audit Office and Public Relations staff. A Deputy Commissioner presides over the unit responsible for the Coordination of European Affairs. There are six administrative divisions (Personnel and Finance; Organization and Outfield; Information Systems, Economics & Statistics; Litigation, Legal Services & Enforcement; European Customs Unit and International Cooperation; and Excises) each of which is managed by an Assistant Commissioner.

The Eurocustoms Consortium, also located within the Paris Headquarters, was created by the fifteen Customs Services of the European Community in order to provide assistance and support to other Customs Administrations, with a focus on those of Central and Eastern Europe.

Customs 'Collections'

---

[*] A handful of overseas Ports of National Interest, as determined by the government, and including the Ports d'Intérêt National des départements d'outre-mer, will remain under state supervision.

[†] Outfield Offices include forty Regional Collections Units and six National Operations and Support Units (*National Intelligence and Investigation Service; National Foreign Trade Statistics Service; National Recruitment and Training Service; Automated Customs Clearance Office; Imports and Exports Permits Bureau; and National Hallmark Service*). For a detailed description of the National Operational and Support Units, please see Appendix 6a.

There are forty Collections Offices (*Directions Régionales*) comprising the 290 ports of entry, 417 preventive branch units and 815 excise offices in France. Each Collections Office is run by a District Commissioner (*Directeur Régional*) and operates within one of the ten regions[*] in France. Each region is run by a Regional Commissioner, who is also responsible for a Collections Office, and is charged with the collection of a percentage of the total anticipated revenue collections of the state. The Deputy Commissioner in each region also serves as the chief of that region's National Intelligence and Investigation Service.

Appointment of Customs Officers

CES is often cited as the most powerful agency in France. With powers rivaling, if not surpassing, the highest ranking officials of the Gendarmerie[†] and National Police Force (*Police Nationale*)[‡], appointments as Customs Officers are highly competitive. In order to attain the status of State Official as a Customs officer, applicants must first pass a rigorous national exam. Once an applicant has passed the initial exam, he or she is invited to enroll in an intensive training program, lasting between four and twelve months, at one of the three Customs Training Institutes of higher education. Throughout the training period, applicants are evaluated by federal officials and training officers and, in the end, must receive a favorable evaluation in order to graduate into the Customs service. Customs Officers, depending on their grade (ranking) and the nature of their responsibilities, may receive promotions based on length of service, internal exams and accomplishments.[341]

Primary Functions

Under French Law, CES assumes three primary responsibilities: the collection of revenue; protection against fraud and crime; and the regulation and facilitation of trade.

> **Revenue Collection** - Each year CES collects tens of billions of euros in revenue. In 2005, a total sum of €60.3 billion was collected, including €42 billion (69.6%)[§] collected on behalf of the central government of France. The remaining 30.4% was collected on behalf of the European Union[**] and local authorities and public entities,[††] comprising €1.6 billion (2.6%) and €16.7 billion (27.8%), respectively.[342]

---

[*] For a list of the ten regions in France and their corresponding districts, please see Appendix 6b.
[†] The Gendarmerie Nationale is France's national military police force run administratively by the Ministry of Defense and operationally by the Ministry of the Interior.
[‡] The Police Nationale is the main civil law enforcement agency in France operating under the jurisdiction of the Ministry of the Interior.
[§] Revenue is comprised of excise duties and taxes; VAT on non-EU state imports; and on hydrocarbon oil.
[**] Revenue is comprised of Customs duties and agricultural levies; compensatory amounts; and sugar levies.
[††] Revenue is comprised of special fees and taxes on maritime transport and the special tax on road fuel collected on behalf of the French "Overseas Departments".

Protection Against Fraud and Crime - CES' second major responsibility is the protection of public security. This is achieved through intelligence operations to combat terrorism and organized crime, security checks in high-traffic areas and imports controls of weapons and ammunition.

On the national level, CES is responsible for enforcing interdictions and restrictions on dangerous materials (*marchandises dangeureuses*), specifically military exports, and regulating international compliance with embargos enacted in the name of international peacekeeping.

Other major components of this role include: intercepting drug-trafficking and money laundering operations; protecting against counterfeiting (money and products violating trademarks); regulating the transport of sensitive goods between EU member states; protecting national French treasures and antiques from theft during transit; protecting endangered species under the Convention on the International Trade in Endangered Species of Wild Flora and Fauna (CITES); controlling attempts at illegal immigration into France; tackling various types of pollution in the name of environmental protection; and serving as the equivalent of the French Coast Guard in French coastal waters and adjacent maritime zones.

Regulation and Facilitation of Foreign Trade - Finally, CES is responsible for regulating and facilitating trade at the local, EU and international levels. At the local level, this role entails: implementing international trade provisions; performing physical and documents controls of selected imports and exports; collecting agricultural levies; and other special charges and handling any payments or refunds to traders.

Outside of its local scope of work, CES is charged with: assessing and collecting duties on non-EU imports as set forth by the Common Tariff of the European Community; compiling and disseminating statistics relating to external trade; running Trade Advisory Units (*Cellules Conseils*) in the interest of expediting trade operations; and establishing close partnerships with airports and seaports to facilitate the flow of merchandise.

Special Provisions/Powers

In accordance with the National Customs Code of France (*Code des Douanes*), the powers conferred upon Customs officers include:

- The Power to search persons, merchandise and conveyances without a warrant or need for reasonable suspicion or probable cause, at the border and at the extended border, at Customs offices, in bonded warehouses, railroad stations, airports, seaports and, more generally, in all open public areas throughout the French territory;[343]

- The power to stop and search vehicles anywhere on French territory, without a warrant or need for a reasonable suspicion or probable cause;[344]

- The power, subject to prior information of the Public Prosecutor and to the consent of the owner, to conduct a search (without a warrant) of business premises for merchandise and/or papers;[345]

- The power to search residential premises, with the assistance of a judicial police officer without a warrant when a violation is being or has just been committed; or subject to a search warrant issued by the president of the *'Tribunal de Grande Instance*[*] in all other cases;[346]

- The power, without serving a subpoena, to command any person involved in matters falling under the regulatory authority of Customs to produce any files, books, records, documents, etc., relevant to the case under investigation[347]; those items are liable to seizure without a warrant; failure to comply is punishable by law;[348]

- The power, subject to the prior authorization of the Public Prosecutor, to conduct controlled deliveries of narcotic drugs or chemical precursors;[349]

- The power to enforce Customs laws and regulations on any vessel within the territorial sea and to prevent or punish infringement of Customs laws and regulations by any ship within the contiguous zone;[350] 1,000 gross ton vessels (or under) may be boarded and searched at sea without any warrant;[351] and others can be diverted to a port for any appropriate action[352]

- The power, subject to the prior authorization of the Public Prosecutor, to board and search a vessel (French, stateless or flying the flag of a cooperating country) in the high seas or to divert it to a port, pursuant to article 17 of the United Nations Convention against illicit traffic in narcotic drugs and psychotropic substances done at Vienna on the 20th of December 1988;[353]

- The power, subject to advising the Public Prosecutor, but without any subpoena being served, to require from currency exchange businesses (non-bank financial institutions engaged in the immediate exchange of money into foreign currency) the presentation of their transaction records as well as of any relevant business paper;[354]

- The power to enforce immigration regulations at the extended land border with neighboring European countries party to the Schengen Agreement as well as at international airports and seaports, subject to advising the Public Prosecutor without delay when an illegal immigrant is being detained and to his being handed over to a judicial police officer within three hours;[355] and

- The power to detain persons and items reported in the 'Schengen Information System,' subject to advising the Public Prosecutor without delay and to their being handed over to a judicial police officer within three hours.[356]

---

[*] Roughly equivalent to a U.S. District Court.

CES also enjoys significant discretion in terms of prosecuting Customs offenses and violations. It may choose not to prosecute; to compound the offenses and deal with them via an out-of-court settlement; prosecute (which under French law implies the "institution of fiscal proceedings" without referring the case to the Public Prosecutor); or request further investigation of the offense by the Public Prosecutor. Judicial powers, in fact, have been awarded to a number of Customs Officers, affording them the status of Judicial Customs Officers (*Officiers de Douane Judiciare*.) In the event that a Customs Officer requests the presence of a Public Prosecutor or an Examining Magistrate, he or she is empowered to conduct a judicial investigation* and to enforce:

- Provisions of the Customs Code;
- Provisions of Excise statutes; and
- IPR Code on Trademarks.

Finally, in the event of a Customs offense involving narcotic drugs, arms and/or stolen cultural goods, the aforementioned judicial investigations are carried out within special ad hoc Customs units, where they work jointly with judicial police officers (of either the *police* or the *gendarmerie*). The Special Agent in charge of these temporary units, as appointed by the Public Prosecutor or Examining Magistrate, can be either a Customs officer or a judicial police officer.[357]

Port Case Study - Marseille

General Port Information

Situated on the French Mediterranean seacoast, the Port of Marseille Authority (*Port Autonome de Marseille - PAM*) operates as a public authority, designated as such in April 1966, and includes the harbor areas of the Gulf of Fos (Port-Saint-Louis-du-Rhône, Fos, Port-de-Bouc and Lavera), of the Etang de Berre, Total La Mede and Shell Berre, and of Marseilles itself.[358] The mission of PAM is to "ensure the construction, maintenance, development and management of the public land entrusted to it, by the decree that created it."[359]

PAM is physically divided into two distinct docks (*bassins*): The Eastern Docks - composed of the harbor areas of Marseille, and the Western Docks (including PAM's main container terminal, Darse 2), comprising Lavéra, Port de Bouc and Port Saint Louis du Rhône[360].

"At the crossroads of the African and South European Zones, PAM constitutes the most important gateway for oil in the South of Europe."[361] PAM is currently the world's third-largest oil port, following the Ports of Houston and Rotterdam. The harbor area

---

* Specific powers for the judicial investigation are detailed within France's Code of Criminal Procedure. If however, a Customs Officer, while conducting a judicial investigation, exercises powers afforded him/her under the Customs Code, evidence obtained is subject to exclusion in French courts.

housing the container terminal at Fos can receive the largest vessels in the world. The Darse 2 terminal boasts five berths for receiving vessels over a 1,777 meter-long dock with a water draught of 14.5 meters; with a total traffic of 92,400,000 tons, PAM is by far, the largest port in France.

As of December 31, 2005, the Lloyd's Register-Fairplay World Shipping and Port Index estimated the following approximate annual shipping levels for the Port of Marseille:

Oil and Oil Products:	60,000,000 tons
Liquid Bulks:	3,600,000 tons
Solid Bulks	13,700,000 tons
General Cargo	14,500,000 tons
Containers	800,000 TEUs
Passengers	1,800,000

Port Security

Of more than 15,000 people[362] working within PAM[*], a number of different groups and agencies are responsible for different aspects of surveillance and overall port security. Mr. Guy Janin, the Director of the Port and Mr. Joseph Moysan, the Port Commander, both provide oversight of the port's security chain of command, although they are equally responsible for a number of other daily operations. In addition to these high-ranking federal officials, the port is secured by a permanent team of Customs officers, factions of the local police force and firefighters of Marseille, a contingency of Border Police (*Polices Frontières*) and privately contracted security guards.[363]

The overall physical security system in place within the port appears well-designed given PAM's primary security concerns.[*] According to Port Director, Guy Janin, terrorism is really not a primary concern at PAM; the port's main concern is combating fraud (*la lutte contre la fraude*), which encompasses theft, false cargo manifests, illegal stowaways and, above all, the movement of contraband into and out of France.[364] Examples of physical security measures at the port include surveillance cameras at most points of entry and exit as well as in high-traffic areas of the port; a 12-foot iron fence lining the perimeter of the port; security guards manning all points of entry and some of the exits; and personnel identification and access cards (*badges portuaires*) consisting of a photo, name, title and access areas.[†] A dockworker, for example, working for a specific company, would most likely only have access (per the identification card) to the terminal out of which his/her company operated.

---

[*] This number includes employees operating within the Port, but not employed directly by the PAM. The total number of PAM employees is 1,500.

[*] This assessment is based upon my visit to the port in March 2006.

[†] It should be noted, however, that persons not working directly in the port but who visit the port on a regular basis (including drivers, handlers, State officers and members of the media) are often issued such cards as well. Further, a person traveling with or accompanying a cardholder does not seem to have to identify his or herself. Finally, though the cards identify which areas or terminals of the port the holder has access to, once inside the port, there is not a subsequent card check to ensure that cardholders are not violating their access restrictions.

Pursuant to the elevation of France's National Security Alert System (*Plan Vigipirate*)[365] to a red alert level[*] in the wake of the 2005 London metro bombings, PAM began reinforcing and strengthening security measures already in place at the port with a particular focus on continuous surveillance and controlling access to the docks (both Marseille and Fos). Since July 2005, random access checks of persons on port premises have increased; no pedestrians can enter the passenger terminal at the port unless they are ticket-holders with valid identification matching the tickets, and the terminal is now only open to the public during transit hours; the parking lot designated for travelers and those coming to pick up passengers arriving at the port is now covered, manned by a security guard and only open during certain hours of the day; and access is restricted in many more areas of the port than it was prior to the announcement of the elevated threat level.[366]

The training requirements for port security officers depend entirely upon the nature of each individual's job and responsibilities. Just as Customs officers have intensive training in their respective areas of expertise, so do the police officers, firefighters and border police operating within the port. Security training for such officers is administered both by the individual agencies for which they work, and by the Port Authority in tandem with the Préfecture[†] of Marseille[367].

In the event of a security incident, every agency tasked with port security has a role to play, these roles are defined in the security plan written by the Port Authority and administered by the Préfecture.

As a final demonstration of its commitment to ensuring the overall security of the port, PAM performed an in-depth analysis of each terminal to determine what extra security procedures and/or devices would be beneficial. These were suggestions for additional terminal security that extended beyond ISPS regulations and were neither promoted nor required by PAM. As a result of this analysis and the subsequent suggestions for improvements, several operators (mostly private) did install new or additional surveillance cameras and hired more security guards for their respective terminals.[368]

Best Practices

Several companies operating at PAM have demonstrated a commitment to increased security via private initiatives and procedures unique to their respective terminals. One in particular, *Manutentionnaires Generale Mediteraneene* (MGM), a French handling company operating at PAM's container terminal, has developed a comprehensive security regime that could be considered a "best practice" at the port.

---

[*] Per the stipulations of France's National Security Alert System, a Red Level calls for measures to be taken against a proven risk of one or more terrorist actions, including measures to protect public institutions and putting in place appropriate means for rescue and response, authorizing a significant level of disruption to social and economic activity.

[†] Each of the 100 Departments in France is overseen by a Prefecture, or governing body. The prefect represents the national government locally and exercises on the local level, the powers that are constitutionally or legally exercised by the national government.

MGM is the largest handling company in Marseille responsible for over 480,000 TEUs annually. Tasked with maintaining containers in such a way that each one is in exactly the same condition when it leaves the terminal as when it arrived, it is critical that MGM's security system be first-rate in order to maintain its competitive advantage at the port. As such, MGM has spent the last eight years creating a system that includes 24-hour surveillance with cameras and a private security detail and a combination of GIS and GPS tracking on all equipment and containers that enter and exit the terminal. All operations are centrally controlled via a randomized pass code-protected computer system called GateExpress, but the system is operated on a terminal-wide WiFi network so that no individual machine or piece of equipment that is tampered with or compromised can lead to a complete system malfunction.

ISPS at the Port of Marseille

France is in full compliance with the mandatory section (Part A) of ISPS and, under the Directive of the EU, also adheres to certain specifications of the voluntary section (Part B). As such, ISPS training and official audits are conducted on a routine basis. Since France's implementation of ISPS in 2004, there have been at least ten audits of various ports and key participants in port security, two of which, were performed by France's First Class Administrator in Chief of Maritime Affairs and ISPS Code Director, Bruno Vaccà.

In an interview with Mr. Vaccà, he stated that "there will be always be inherent vulnerability in maritime security, any kind of security for that matter."[369] Vaccà further offered, however, that ISPS is as comprehensive a code as can possibly be implemented effectively right now to address international security concerns and he didn't identify any glaring weaknesses or holes in the code to be addressed immediately. In fact, for the most part, Vaccà believes ISPS has been received favorably by France's key maritime security actors.

Currently, no state or EU funding is being offered to port authorities or companies operating within the ports, to help defray the costs associated with the implementation of or adherence to ISPS. The financing falls completely on the shoulders of port operators and, though they see the benefits of ISPS in terms of the security of their shipments, they do feel the financial responsibility should be shared by a number of different parties, including the state. Currently, the EU is looking into ways to relieve the operators of some of the financial burden, but the European Commission is unwilling to turn complete financial responsibility over to EU member states. The reason for this is twofold: first, the EU does not want to further burden state budgets; and second, it feels an unfair advantage would be afforded to the wealthier member states.

According to Mr. Vaccà, the implementation of ISPS in France has not, in and of itself, enhanced France's outlook on or commitment to national and international security. France has always been a very security-conscious country and so "it is not as if the introduction of ISPS presented a new concern for French officials and policymakers."[370] It did, however, "re-sensitize" them to the issue, compelling key players to ask themselves if France was doing everything it could and should be doing.

Bruno Vaccà does not find any part of ISPS "limiting" or "inefficient"[371], but that is, perhaps, because the code complements the security apparatus that France already had in place prior to ISPS.

Mr. Vaccà would like the Congress to know that he is pleased that there are always people thinking about and trying to develop better measures and plans for maritime security as it is a "most important and extremely sensitive" issue. He does hope, however, that before the U.S. tries to develop or enact any new legislation that will affect maritime security and port operations on an international level, it will allow the proper time and allocate the proper resources to ensure that everything it has proposed and enacted up to the present, is operating as smoothly, efficiently and effectively as possible.[372]

Customs at the Port of Marseille

There are 670 Customs officers in Marseille, 400 of whom work directly in the port. Of these 400, 270 work on the main (Eastern) dock and the remaining 130 work on the Western dock, harboring Marseille's Container Terminal, Darse 2.

Customs officers are the most influential and powerful actors at the port (in terms of scope of responsibilities and authorizations for action.)* In spite of this hierarchy, there does not seem to be any sort of power struggle occurring between the various agencies responsible for security, as roles and rights are clearly defined and are fairly transparent. According to François Brivet, Co-Director of Regional Customs for Marseille, Customs officers interface and cooperate well with police, firefighters, and port officials, and are particularly committed to sharing information (when possible and appropriate). PAM sees a real sense of cooperation and interdependency among agencies.[373]

Customs conducts a number of different kinds of inspections at the port including document and declaration checks (made easier and more efficient with the initiation of the 24-hour rule);[374] physical inspections of trucks and transit equipment; random security checks and inspections of traveling passengers; container inspections using PAM's new x-ray scanner (purchased in order to become fully CSI-compliant); and a large number of hand-held radiation detectors.† For the purpose of this study, the container scans are the most important inspections being conducted at the port.

The relatively new HCV-Mobile System x-ray scanner, purchased by PAM‡ from Smiths Detection, and implemented in June 2005, can scan between 10 and 18 containers per hour and can penetrate up to 270mm of steel in order to receive images at the bottom of fully loaded container trucks. The scanner, which is installed at the FOS

---

* Customs is the only agency dealing with port security with the power to survey and check merchandise that is in transit, without a warrant.

† These became extremely widespread throughout European ports, following the 1986 incident at Chernobyl.

‡ The HCV-Mobile Scanner was purchased for approximately 3 million euros (roughly 3.67 million dollars) by the PAM. The funds were raised by the PAM in order to fund the purchase by levying annual prices across the board, at the Port.

Container Terminal, Darse 2, scans approximately 600,000 containers per year; roughly one fifth of these are bound for the U.S.[375]

CSI

PAM is one of two Container Security Initiative (CSI) compliant ports in France; the Port of Le Havre is the other compliant port. On January 7, 2005, PAM became the 34th operational port under the CSI agreement. Only months later, two U.S. Customs and Border Protection agents were placed at the FOS Container Terminal at the Port's Western Docks. The agents, who were received under the December 3, 1993, Franco-American Convention on Mutual Administrative Assistance (*Convention relative à l'Assistance Administrative Mutuelle*), have been residing and working at FOS since the summer of 2005. One agent has already completed a full rotation and was recently replaced at the port. Overall, U.S. CBP agents stationed at FOS have been satisfied with the thoroughness of French Customs cargo inspection.[376] There have been very few instances in which a CBP agent has requested an inspection that French Customs had not planned on performing, and when requested, French Customs has complied. In addition to the agents stationed at FOS, PAM has taken full advantage of the mutual nature of CSI, having sent a French Customs agent to New York to help monitor exports headed for France. The major French enterprises involved in maritime transport have already realized the benefits of this exchange - particularly in terms of commercial development - and, so far, relationships between French and American agents have been amicable. As such, French Customs is interested in maintaining an ongoing agent exchange program between France and the U.S.

Since becoming CSI-compliant and receiving U.S. CBP agents at the port, PAM has apprehended a large, illegal shipment of cigarettes to Italy. No seemingly terrorist-related shipments or incidents have arisen.[377]

Though the actual implementation of CSI in the port has predominantly fallen under the jurisdiction of French Customs, the high costs of implementation have affected the entirety of France's maritime supply chain. In addition to costs to conduct terminal security assessments, install additional equipment, hire additional security personnel and purchase a new scanner, shippers, handlers, transporters and terminal operators are all bearing the costs of actual container inspections.

According to Customs' Francois Brivet, every container scan, whether conducted for CSI or for regular in-bound trade, incurs a cost of €150 to €200 ($180 to $240), which must be paid by the terminal operator. Should a scan be deemed insufficient, the container is physically opened and emptied – at an additional cost of €1,500 ($1,800). Containers are selected for scans and physical inspections based on such factors as Customs intelligence reports, the security history of the shipping company responsible or its transport, whether the container is for import or export and its point of origin or destination.[*]

---

[*] Most containers that will be scanned are predetermined even before they arrive at the port, as Customs has their information 24 hours in advance of their arrival, per ISPS' 24-hour rule.

As a means of defraying all of these costs, PAM has raised its annual prices across the board and instated an additional surcharge for handling companies. Shippers operating at the port have raised their prices as well. As a result, the price of container shipments has increased by €8 to €40 ($10 to $50) per container.

Finally, as every actor at every level in PAM's maritime supply chain has been affected in some way by Marseille's implementation of CSI, everyone has, and wants to express, an opinion. For a complete listing of responses to and opinions on CSI from major transit companies, shippers, handling companies, French Customs, and the Port Authority, refer to Appendix 6c.

Lessons Learned and Conclusions

As the largest port in France, with both proximity and ties to the Middle East and North Africa, the Port of Marseille Authority is a critically important component of the post-9/11 security initiative to push U.S. borders out.

Historically, PAM has not been overly concerned about terrorist activities, choosing instead to focus security efforts on combating fraud (theft, stowaways, false manifest and contraband). In the last five years, however, U.S. and international pressures to increase port security on an international scale, has forced a shift in security priorities at the port. Today, PAM is a much more secure entity, both overall and within its individual terminals. It is better prepared for a terrorist attack and better equipped to detect and prevent such an attack from occurring. This preparation and the newly implemented security initiatives have come at a very high price to the port and its clients and few, thus far, have been convinced that the investment was the best allocation of the port's resources. Port officials will continue to adhere to increasingly stringent international security practices and regulations so as not to interrupt international trade, but overall security priorities at PAM will remain focused on combating fraud.[378]

Key actors in charge of maritime security in France and, more specifically at PAM, are generally satisfied with the most recent international security initiatives and feel they have been implemented in an efficient, effective way. ISPS is considered a timely, comprehensive measure that benefits companies and entities operating at all levels of the maritime supply chain. For entities such as PAM, whose security procedures were fairly advanced to begin with, ISPS serves to complement and enhance existing security. Port operators, though, continue to express a desire for a more equal distribution of ISPS costs across the supply chain. CSI, on the other hand, has yet to be appreciated by anyone other than French Customs. Most of the port actors interviewed during the site visit shared the opinion that CSI was not only unilaterally crafted by the U.S., but also that it is beneficial only to the U.S. Interviewees felt that the initiative had been extremely costly and not particularly worthwhile, but that to not participate would have been even more costly in the long run. A shared consensus was that the initiative seriously compromised the fluidity of the maritime industry, particularly during the first months of its implementation at a port, and that a "seemingly" more secure supply chain was not worth the risk.

In an age of global interdependence plagued by declining religious, political and international tolerance, enhancing the security of the international trade community at large is a universal priority. France has gone above and beyond the basic requirements of ISPS and has worked hard to certify its two largest and most internationally significant maritime ports as CSI-compliant. In return, the entities involved in France's maritime sector request that the international initiatives that are already in place be refined and harmonized from port to port and country to country before developing or executing any new initiatives. Furthermore, they hope to see less of a unilateral approach to the creation and implementation of such initiatives and an increase, across the board, of intelligence-sharing and communication.

Appendix 6a

French Customs: National Operational and Support Units

Unit 1: National Intelligence and Investigation Service *(Direction Nationale du Renseignement et des Enquêtes Douanières)*
Location: Headquartered in Paris with 12 additional field offices throughout France
Responsibilities: collection, analysis and dissemination of intelligence and for major investigations into matters arising through the entire French territory from the main businesses of the Department (Customs, Excise, some aspects of VAT)

Unit 2: National Foreign Trade Statistics Service (*Direction Nationale des Statistiques du Commerce Extérieur*)
Location: Toulouse
Responsibilities: Monthly publications of France's foreign trade statistics

Unit 3: National Recruitment and Training Service (*Direction Nationale du Recrutement et de la Formation Professionnelle)*
Location: Neuilly
Responsibilities: Organization of entrance exams to determine Customs Departmental Classes (Administrative, Executive and Clerical); organization of selection tests for promotion to supervisory and management posts; and training specialists. This Unit is supported by three Customs Academies (Neuilly, La Rochelle, Rouen) and by Training Liaison Officers in the Collections.

Unit 4: Automated Customs Clearance Center *(Centre Informatique Douanier)*
Location: Osny
Responsibilities: Operation and maintenance of the French Customs Automated Commercial System known as "S. O. F. I." (Système d'Ordinateurs de Fret International).

Unit 5: Import and Export Permits Bureau *(Service des Titres du Commerce Extérieur)*
Location: Paris
Responsibilities: The issuance of most Import and Export Permits required under French legislation

Unit 6: National Hallmark Service *(Direction Nationale de la Garantie et des Services Industriels)*
Location: Headquartered in Paris with a number of field offices throughout France
Responsibilities: Accuracy assessment and certification of a variety of metrological instruments; and stamping French official marks on precious metals.

Appendix 6b

French Customs: Regional Breakdown of France

Region I: Antilles-Guyane (Fort-de-France, Martinique, FWI): *Districts of Guadeloupe, Guiana and Martinique*

Region II: Bordeaux: *Districts of Bayonne, Bordeaux and Toulouse*

Region III: Burgundy (Dijon): *Districts of Besançon, Dijon and Orléans*

Region IV: Île-de-France (Greater Paris*): Districts of Downtown Paris, Eastern Paris, Western Paris, Orly and Roissy (CDG-Airport)*

Region V: Lille: *Districts of Amiens, Dunkerque, Lille and Valenciennes*

Region VI: Lyons: *Districts of Annecy, Chambéry, Clermond-Ferrand and Lyons*

Region VII: Provence-Alpes-Cote d'Azur et Corse: *Districts of Aix-en-Provence , Ajaccio, Marseilles, and, Nice*

Region VIII: Metz: *Districts of Metz, Mulhouse, Nancy, Reims and Strasbourg*

Region IX: Pays-de-la-Loire (Nantes): *Districts of Nantes, Poitiers and Rennes*

Region X: Rouen: *Districts of Caen, Le Havre and Rouen*

Region XI: Languedoc-Roussillon: *Districts of Montpellier and Perpignan*

Appendix 6c

Opinions on the U.S. Container Security Initiative

The statements below are a compilation of direct quotes, translated from French into English, from interviews conducted in Paris and Marseille, France with members of the shipping industry, as well as government officials involved in maritime and port security.

- Both shippers and handlers charge an extra fee now for CSI compliance costs—this ends up being very profitable for all sides

- Pre-declarations become very difficult as the declarations must be made even before anyone has had a chance to verify the true nature of the cargo

- We really sense that CSI is a completely American-imposed initiative with no real benefits to anyone except the U.S.

- CSI doesn't work everywhere even when people say it is working: For example, at the Port of Le Havre, Customs has setup a different system and not everything is declared in the same manner as at other autonomous ports- simply because of the arrangements made by Customs officers with various ports.

- For safety purposes, CSI is not best practice because, although the shipper knows what's in the containers/shipments, the Customs officers in the ports don't know until the cargo actually docks in the Quay.

- We (the shipping community) need to be able to follow merchandise while it's in transit. We care less about port-specific checks, whether they be in the port of departure or port of arrival.

- Things need to be done and implemented more slowly—(tracking, for example) we can't just raise prices all of a sudden for terrorist prevention when the entire [French] community's main priority is contraband.

- Globally, CSI seems to be a good initiative but it poses a lot of problems for those people who have to adhere to it in terms of technical and financial problems not to mention the fact that it really slows down maritime transport until each company, each agent, and each port has got a really good grasp on everything new.

- It is very important, when implementing a new security measure that affects everyone involved in maritime transport that [the U.S.] not completely do away with the fluidity of the industry, in exchange for a seemingly more secure supply chain.

- Technically speaking, to secure a container is not an easy task. Perhaps the tracking element of CSI for each container is not necessary and should be applied in certain instances, with certain types of cargo only.

- It is time to stop acting in such a (seemingly) unilateral manner. These initiatives CAN be good for securing all countries, but should be undertaken and implemented by international organizations.

- We have yet to see the difference in port treatment between CSI compliant and non-compliant ports.

- It is very important that the US Administration begin to really work with the shipping industry and stop acting unilaterally with security initiatives.

- CSI Ports are really not any better regulated or secured than non-compliant ports, it's really ISPS code that makes everything work well and efficiently. Apart from the scanner (which really seems to just add one more layer of security on the exact same thing)—the only real difference between CSI and non-CSI is the fact that American Customs can come audit.

- [We] don't think that the presence of American customs agents at the port works any better than just making sure there is good cooperation and communication between country customs officers.

- The U.S. is looking too hard for comparisons between air and maritime transportation but they are two very different industries with very different supply chains and one is about cargo and the other is about human passengers—so security cannot be handled in the same way. We (at the port) are much more concerned-in terms of terrorism- about cruisliners docking at the port than we are about container shipments.

- In order to harmonize the security at ports in the system, it is important to use the resources we have already set in place, but not yet perfected (if we had, we wouldn't be looking for alternatives) like ISPS and do things like increase intelligence sharing between international agencies; educate all citizens on their responsibilities (not just the people in the ports) so that every citizen becomes an actor in security. Make ISPS (all parts) mandatory – realize that Customs is *one* aspect of the security chain, not the entire thing- everyone has a role. We need a change in mentality, not more rules.

- Intelligence is everything. If we don't have cooperation and intelligence sharing, then none of these codes and initiatives means anything.

Chapter 7. Hong Kong and the Port of Hong Kong

Introduction

Located at the southern tip of China and bounded by the South China Sea, Hong Kong is a Special Administrative Region (SAR) of the People's Republic of China. As such, this chapter pertains only to the laws and practices of Hong Kong, and not to those of mainland China.

Following its return to China in 1997, Hong Kong was granted SAR status, which allows it to retain a "one country, two systems" arrangement with China. Under this arrangement, Hong Kong was permitted to retain its open political and economic system, and relative autonomy in most affairs. With a small geographic area of only 1,042 sq km, but a large population of 6,898,686 (July 2005 est.), Hong Kong depends on trade for its economic survival. In 2005, imports totaled US$291.6 billion* and exports totaled $286.3 billion, with almost half of all imports and exports coming from and going to mainland China.[379] As China's share of global manufactured goods has increased over recent years, Hong Kong has exported increasing flows of Chinese goods to the rest of the world. Currently, over 70% of all Chinese exports leave through the Port of Hong Kong.[380]

General Port Information

The Port of Hong Kong occupies a strategic position in the South China Sea, lying at the mouth of the Pearl River Delta.[381] A naturally sheltered, deep-water port, "Hong Kong possesses one of the most perfect natural harbors in the world."[382] The Hong Kong Region boasts over 200 islands and 733 km of coastline.[383] Victoria Harbor covers an area of 4,900 hectares, and ranges between 1.2 and 9.6 km in width.[384] In recent years, however, limited availability of land has led the Hong Kong government to reclaim much of the harbor for development projects.

In 2004, the Port of Hong Kong was the busiest container port in the world, a position it has held for 12 of the past 13 years.[385] In the same year, the port handled 22.0 million TEUs (twenty-foot-equivalent units); the Kwai Chung and Tsing Yi Container Terminals handled 13.4 million TEUs of this throughput, while 8.6 million TEUs were handled by mid-stream and smaller terminals.[386] A total of 35,900 ocean-going vessels passed through Hong Kong in 2004, with an average turnaround time of 13 hours for container vessels.[387]

The Port of Hong Kong houses several types of terminals. The largest volume of trade passes through the nine container terminals, while increasing volumes of transshipment goods from China flow through the mid-stream and river trade terminals. A number of smaller terminals support ferry traffic, cruise vessels, and the shipment of raw goods.

---

* Unless otherwise noted, all currency is listed in U.S. dollars.

Container Terminals

Hong Kong has nine container terminals, located at Kwai Chung and Tsing Yi. The terminals have a total of 24 berths with 8,500 meters of frontage and a total throughput capacity of 18 million TEUs.[388] * The terminals are run by the following four private terminal operators:

Modern Terminals Ltd. (MTL) – MTL operates terminals 1, 2, 5 and the southern part of Terminal 9. The terminals include 7 container berths and 2 feeder berths, and have a stacking capacity that exceeds 51,100 TEUs.[389] Modern Terminals was established in 1969, and is one of the two largest terminal operators in China.[390] †

Dubai Ports International Terminals (DPI) – DPI owns Terminal 3, with one berth, and Terminal 8 (West), with two berths. Terminal 8 is operated by Asia Container Terminals Limited, of which DPI is the principal shareholder. DPI was founded in 2001, and has achieved rapid, double-digit growth since its inception.[391]

Hong Kong International Terminals (HIT) – HIT operates Terminals 4, 6, and 7, as well as two berths of Terminal 9 (North). HIT's terminals contain a total of 10 ship berths, 4 barge berths, and a stacking capacity that exceeds 76,000 TEUs. HIT is the flagship operation of Hutchison Port Holdings, the world's largest, private port operator.[392] In 2004, HIT and COSCO-HIT (a joint-venture terminal between Hutchison and COSCO Pacific) handled a throughput of 7.452 million TEUs, constituting over 50% of Kwai Chung's container traffic.[393]

COSCO-HIT - COSCO-HIT operates Terminal 8 (West), which houses 2 container berths, with a stacking capacity of 18.25 TEUs.[394] COSCO-HIT is a joint-venture formed by COSCO Pacific Ltd. and Hong Kong International Terminals.[395]

River Trade Terminals

The Hong Kong River Trade Terminal facilitates barge shipments of containers and bulk cargo between Hong Kong and mainland China ports in the Pearl River Delta. The terminal is owned and operated by Hutchison Port Holdings; it contains 49 barge berths, and has an overall area of 65 hectares.[396] The terminal was completed in 1999, and serves a growing volume of transshipments between Hong Kong and the Pearl River Delta.[397] The importance of Hong Kong-China river trade is only expected to increase

---

* The Hong Kong Port Development Council and the Hong Kong government are currently negotiating plans for a 10th and 11th terminal. Northwest Lantau Island or Southwest Tsing Yi have both been named as potential locations for the 10th terminal. The addition of both terminals is part of the Hong Kong Port Master Plan 2020.

† Modern Terminals' shareholder portfolio is comprised of the following companies: The Wharf (Holdings) Limited (68%); China Merchants Holdings (International) Co Ltd (27%); and Jebsen Securities Ltd (5%).

in the coming years, due, in part, to a new pan-Pearl River Delta trade block formed between Hong Kong and nine Chinese provinces.[398] *

Mid-Stream Terminals

Hong Kong's mid-stream facilities primarily serve to load and unload cargo from barges to trucks and lorries and vice versa, moving between Hong Kong and mainland China. Currently, these facilities are situated in 11 different locations occupying a total land area of 27.5 hectares and water frontage of 3,197 meters.[399] Approximately 25% of cargo shipments and 37% of container traffic are handled at mid-stream operations.[400] An estimated 20,000 to 30,000 containers arrive daily in the Hong Kong port from mainland China.[401] One of the largest mid-stream operators in Hong Kong is Asia Port Services, a subsidiary of Hutchison Port Holdings. Mid-stream operations have become increasingly popular, as they provide a "low-cost alternative to both the smaller ships carrying Intra-Asia cargoes, and the mid-size ocean going ships including Intra-Asia and trans-ocean line hauls."[402]

Miscellaneous Port Terminals and Facilities

The Port of Hong Kong is home to multiple other facilities, including:[403]

- Bulk handling facilities for coal and oil located at Castle Peak and Lamma Island;
- Public cargo working areas maintained by the Marine Department to facilitate the transfer of cargo between vessels and shore, and to and from Pearl River ports;
- The Macau Ferry Terminal, providing ferry service to Macau, and the China Ferry Terminal, providing ferry service to 16 mainland China ports;
- The Ocean Terminal, with 2 berths that can accommodate passenger cruise liners; and
- Numerous terminals used for shipments of raw and finished materials such as petroleum, chemicals, cement, and oil.

Port Administration

The Port of Hong Kong does not have a Port Authority charged with oversight and control of port infrastructure. Because all port facilities in Hong Kong are privately owned, government interference with facility operations is minimal.[404] The Hong Kong Marine Department serves as the primary government authority at the port, while the Economic Development and Labour Bureau provides general oversight and planning for port development. In addition, numerous public/private councils and committees serve

---

* The newly established trade block aims to "lower trade barriers among members, standardize regulations, and improve infrastructure".

in advisory capacities at the port. Overall, the private sector is afforded a great deal of input and control in port activities.

Government Agencies

Economic Development and Labour Bureau

The Economic Development and Labour Bureau is responsible for the development of Hong Kong's infrastructure. Within the Economic Development Branch of the Bureau, the Deputy Secretary for Economic Development and Labour, Miss Janice Tse, heads the division that oversees Port Development and Logistics. She is assisted by Mr. K.M. Fung, Chief Assistant Secretary for Port, Maritime and Logistics, and Miss Winky So, Principal Assistant Secretary for Port, Maritime and Logistics. This division is charged with formulating maritime policy, coordinating long-term port development planning, and "provid[ing] a conducive environment and [the] necessary infrastructure to facilitate the development of the logistics sector, and to maintain Hong Kong as the preferred regional transportation and logistics hub."[405]

Marine Department

The Hong Kong Marine Department serves as the government authority over the Port of Hong Kong, and falls under the jurisdiction of the Secretary for Economic Development and Labour.[406] The primary functions of the Marine Department are "to ensure safe operation of the port and all Hong Kong waters as well as to operate the Hong Kong Shipping Register and safeguard the quality of the Hong Kong registered ships."[407] The Department's mission states, "We are One in Promoting Excellence in Marine Services."[408]

The Marine Department is headed by the Director of Marine, Roger Tupper, followed by the Deputy Director of Marine. Below the Deputy Director are the five main divisions of the Marine Department, each of which is headed by an Assistant Director who reports directly to the Deputy Director. The five main divisions include Port Control, Planning and Services, Multilateral Policy, Shipping and Government Fleet, and their functions are described below:[409]

> **Port Control Division** – Port Control is responsible for all Port Operations Procedures, including the entry and exit of vessels; licensing and control of local vessels; and port services such as maritime search and rescue, traffic control, and vessel safety.[410]
>
> **Planning and Services Division** - Planning and Services is in charge of "strategic planning for port development, passenger terminals, pollution control, public cargo handling facilities, buoys and navigational aids, hydrographic services."[411]
>
> **Multilateral Policy Division** - The Policy Division is charged with the development of all standards and legislation that regulate local and international shipping, maritime security, and environmental protections. This division serves

as a liaison between the shipping industry and other government bureaus in order to facilitate compliance with any changes to shipping or security legislation.[412]

Shipping Division - The Shipping Division oversees the enforcement of local and international shipping standards, and conducts surveys, examinations, and certifications of both ships and their crews.[413]

Government Fleet Division – The Government Fleet Division is responsible for all tasks related to the "procurement, maintenance, operation and crewing of government vessels."[414]

In addition to the five primary divisions, Marine Adviser W.K. Lee serves as Hong Kong's representative to all international assemblies relating to maritime issues.[415] *

Non-Government and Public/Private Agencies

Non-government agencies and public/private entities play a significant role in Hong Kong's port operations and maritime security. These include the Hong Kong Port Development Council, the Hong Kong Maritime Industry Council and the Marine Department Advisory Councils. Agency functions are outlined below.

Hong Kong Port Development Council (PDC)

The PDC advises the Chief Executive on all aspects of port planning and development. It also coordinates "the involvement of government and private-sector agencies in the planning and development of the port services."[416] The PDC is chaired by the Secretary for Economic Development and Labour, and its membership is composed of both government and private officials.

Hong Kong Maritime Industry Council (MIC)

The MIC serves as an advisory council to the Economic Development and Labor Bureau. The purpose of the MIC is to advise the Bureau on the "formulation of measures and initiatives to further develop Hong Kong's maritime industry."[417]

Marine Department Advisory Councils

The Marine Department has 11 advisory committees composed of both public and private members, including:

- Committee on Boating and Yachting;
- Consultative Committee on Ship Personnel and Management;
- High Speed Craft Consultative Committee;
- Mercantile Marine Assistance Fund Committee;

- Pilotage Advisory Committee;
- Port Area Security Advisory Committee;
- Port Operations Committee;
- Port Welfare Committee;
- Provisional Local Vessels Advisory Committee;
- Seafarers' Advisory Board; and
- Shipping Consultative Committee.

Port Security

As the world's busiest port, Hong Kong officials recognize that good port security is critical to the port's continued competitiveness as a global trading hub. Most of Hong Kong's security concerns thus far have revolved around smuggling and human trafficking. Hong Kong does not have any local terrorist groups, nor is it considered at high risk for local terrorism. As a major world port, however, Hong Kong officials remain concerned about regional terrorism, and the possibility of a security incident occurring on a ship passing through Hong Kong's territorial waters.[418] Fortunately, Hong Kong has not experienced any major security incidents since its implementation of ISPS.[419]

General Security Procedures

Any vessel arriving in Hong Kong waters, or intending to continue through to mainland China ports must provide pre-arrival notification 24 hours in advance. If port security levels are raised, additional notification time may be required.[420] Should a vessel be deemed a threat or concern, the vessel would not be boarded prior to entering Hong Kong waters; instead, it would be denied entry by the Marine Department.[421] In the event of a security incident within Hong Kong's jurisdiction, the Marine Department's Marine Emergency and Maritime Rescue Co-Coordination Centre would coordinate the response of all involved government agencies.[422]

Because all container terminals are privately owned at the Port of Hong Kong, each terminal operator is responsible for security at its own facilities. Per ISPS, each terminal has appointed a Port Facility Security Officer (PFSO) and has implemented a Port Facility Security Plan (PFSP).[†] All Hong Kong container terminals use state-of-the-art access controls, including fencing, CCTV, patrols, and identity cards.[423] Many facilities were already using this technology prior to ISPS implementation; however, since implementation, additional upgrades have been made.

---

[*] Mr. Lee serves in the Hong Kong Economic and Trade Office, located in London, England.
[†] All Port Facility Security Plans are confidential and proprietary. Their details cannot be released to any outside agents.

As one of Hong Kong's busiest terminal operators, HIT provides an excellent example of best practices for private terminal security. HIT has 9 deputy Port Facility Security Officers, and a large staff of lower-level security officers. The company provides a staff of full-time, in-house security officers, as well as contract officers.[424] HIT is in the process of upgrading its CCTV system, and adding additional perimeter fencing for intrusion detection. All terminal gates are guarded, and access to containers is controlled both land-side and water-side. All entering trucks must pass a verification procedure, and in addition, all approved truck drivers must present Truck IDs for any pick-ups and deliveries.[425]

Government Agencies Involved in Port Security

All port security issues fall under the general jurisdiction of the security bureau, and specifically under the jurisdiction of the Secretary of Security, Mr. Ambrose Lee Siu-kwong. Government agencies involved in overall port security include: the Port Area Security Advisory Committee, the Port Facility Security Working Group, the Hong Kong Police and the Immigration Department. Agency functions are outlined below:

Port Area Security Advisory Committee (PASAC)

PASAC was created in July 2003, and is chaired by the Deputy Director of Marine. The committee serves in a consultative capacity, tasked with advising the Marine Department "on all matters relating to the implementation of the IMO International Ship and Port Facility (ISPS) Code in the Hong Kong Special Administrative Region including port area security requirements, ship/port interface matters and to monitor the application of ISPS Code after 1st July 2004."[426] *

PASAC's membership includes representatives from the Marine Department, the Hong Kong Police Force, the Hong Kong Container Terminal Operators, Oil Terminal Operators, Ship Repairs Industry, River Trade Terminal Operators, the Hong Kong Liner Shipping Association, the Cruise Industry, and the Bulk Industry.[427]

Port Facility Security Working Group (PFSWG)

The PFSWG was formed on July 11, 2003, with representation from the Marine Department, the Customs & Excise Department, Immigration, and the Hong Kong Police.[428] The PFSWG is an interdepartmental working group, which serves as the executive arm of the Marine Department in enacting port security requirements outlined by ISPS. In addition, the PSFWG has "the responsibility of assisting port facility operators to carry out their own security assessments and prepare security plans" for approval by the Marine Department.[429] †

---

* The primary focus of PASAC is port security, as opposed to ship security, although the security of port-ship interfaces is considered.

† The Chairman of the PFSWG is Mr. K.M. Fung.

Hong Kong Police Force

The Hong Kong Police Force is charged with first response to any security breaches or issues that arise in terminals or at sea. The land police respond to land-side security, while the marine police respond to water-side issues.[430] In addition, Hong Kong Police maintains a Special Forces unit specifically trained to handle counter-terrorism activities should a major security event occur on sea or land.[431] * The primary task of the Marine Police is to prevent illegal immigration or smuggling at sea.[432] † The Marine Police maintains a fleet of 145 water craft, some of which are equipped with thermal imaging and electronic navigational aids, in order to assist in nighttime operations.[433] In addition, the Police Force advises the Marine Department on the proper settings for port security levels.

Immigration Department

Immigration clears incoming and outgoing passengers and cargo. Cargo is cleared at one of three anchorages: Western Anchorage, Eastern Anchorage, or Tuen Mun Anchorage. Passengers receive clearance at the China or Macau Ferry Terminals.[434] Because of the size of Hong Kong's port, sea entries are common for incoming visitors. In 2002, approximately 20.3 million people entered Hong Kong by sea.[435] These numbers underline the importance of adequate maritime security.

Private Security Initiatives at the Port of Hong Kong

In 2004, the Hong Kong Container Terminal Operators Association (HKCTOA), in conjunction with Science Applications International Corporation (SAIC), undertook a pilot project for container screening.‡ *The Integrated Container Inspection System* (ICIS), funded privately by the HKCTOA, was undertaken as an effort to seek out new and innovative approaches to container security, above and beyond the minimum requirements of ISPS.[436]

According to John Kok of Hutchison Port Holdings (HPH), the project, though expensive, is clearly in the "enlightened self-interest" of the companies involved.[437] In fact, although Hutchison International Terminals, and Modern Terminals Ltd. are competitors, both companies worked together to install the ICIS technology at their terminals. Both operators insist that security must be viewed as a non-competitive issue.[438]

HPH sees the pilot project as only one step in its ongoing work to secure the global supply chain. In Kok's view, security of facilities is important, but inadequate, without a

---

* Due to Hong Kong's long-standing relationship with Britain, the Special Forces unit still receives training from Britain's Special Forces.

† Smuggling remains an issue of great concern in Hong Kong, and has been a longtime maritime security issue.

‡ The HKCTOA is a private organization, comprising members of all four of Hong Kong's container terminal operators.

multi-layered approach to security of the entire supply chain. All parties involved in container security should be concerned with two essential questions: 1) what's inside the box; and 2) did anyone compromise the integrity of the container? Answering these two questions will require multiple layers of security. These layers include security not only at port facilities, but also through the use of trusted parties and increased access to information. Hong Kong's pilot project aims to aid security in this first layer, security at the port facility.[439]

The ICIS technology was developed by SAIC and offers a method for scanning all incoming and outgoing containers without impeding the flow of traffic. At HIT, containers are being scanned at the gate while at MTL a pair of scanners can scan containers at the gate or on the quay itself. The advantage of the mobile scanner is that it allows the terminal to scan transshipment containers that arrive by barge.[440] The increasing volume of barge traffic flowing through non-ISPS compliant mid-stream terminals emphasizes the importance of such mobile scanners.

In order to achieve the most complete and accurate data possible, ICIS combines three different types of scans. First, containers pass through the VACIS gamma-ray imaging system, which provides a radiographic image of the container's contents.[441] The advantage of a gamma-ray system over an x-ray scan is its facilitation of a speedier inspection process.[442] * The VACIS system takes a moving scan of the truck, allowing trucks to pass through the scan at speeds of up to 16 km/hour.[443] Though an x-ray scan would provide a higher-powered picture, the scan would require much more time and would impede the necessary flow of traffic.[444] † Additionally, the gamma ray provides a more focused picture, while requiring less power. The higher-powered x-ray would be likely to shoot all the way through the cab of entering trucks.[445]

Second, the "EXPLORANIUM Radiation Portal Monitor (RPM) provides a graphic profile of radioactivity levels inside the container."[446] Finally, the Optical Character Recognition (OCR) system identifies each container's unique ID code, in order to better integrate the data and provide easy electronic data access. Data obtained through the three scans are compiled and integrated into the ICIS database on the main ICIS server. This server offers users secure access to the data from any location in the world.[447]

Thus far, the HKCTOA feels it has been able to prove that the ICIS technology is sound and can be effectively used without compromising the flow of containers through the terminal. To date, HIT has captured over one million scans and more than 20,000 images have been provided to the U.S. government for further use. In addition, MTL and HIT have provided images to various European Customs agencies for their use.[448] HKCTOA believes the advantage of the ICIS technology is clear for Customs agencies.

---

* Use of an x-ray scanner would require a minimum of 2-15 minutes per truck.

† Questions have been raised about the quality of the images obtained through a moving scan. However, according to HPH, representatives from the US Customs & Border Protection, Department of Homeland Security, and the Department of Energy examined the ICIS scans and all supported the adequacy of the gamma ray scan. Should a company find cause for alarm in the gamma ray scan, the truck could potentially be taken to an x-ray facility for a longer, higher-powered scan.

The scans are "capable of providing Customs authorities and other relevant parties around the world with comprehensive, integrated scanning data on every export container that enters a terminal, potentially improving targeting for further inspection and enabling inspectors to target high-risk containers quickly and efficiently by identifying differences from expected contents."[449]

One of the greatest advantages of the ICIS system is its potential ability to provide increased supply-chain visibility to the entire global market. Hong Kong terminal operators believe that widespread implementation of the ICIS system could eliminate the need for a worldwide shutdown after a terrorist threat or incident. Governments and supply-chain owners would be able to track a threatening shipment's movements from beginning to end, and create a targeted shutdown of the necessary areas and facilities. The worldwide economic advantages of such a targeted shutdown cannot be underestimated.[450]

To date, the greatest weakness of the ICIS program stems from a lack of government coordination and cooperation. Although the terminal operators possess the technology to create the scans, governments need to establish joint protocols to assess and respond to all scanned information. Presently, even if a suspicious container was spotted on a scan, no government response procedures are in place.[451] Such procedures need to be established internationally, with the joint cooperation of all governments. Should governments establish varying protocols, or differing radiation thresholds for a response, the security of the whole supply chain could be weakened. Without government support and leadership, the enormous potential of the ICIS project will remain unfulfilled.

ISPS at the Port of Hong Kong

Hong Kong Port Security Legislation

Hong Kong enacted into law the requirements of ISPS and SOLAS amendments with the Merchant Shipping (Security of Ships and Port Facilities) Ordinance and its subsidiary rules. The legislation became effective on June 29, 2004. The ordinance and its subsidiary rules directly reference provisions of Part A of ISPS and chapter XI-2 of the SOLAS convention. They provide a statutory baseline of port security requirements by assigning the basic powers, duties, and responsibilities found in Part A of ISPS. The legislation is not as comprehensive as its American counterpart, the MTSA, and does not provide as detailed a description of the roles and responsibilities of the stakeholders.

The ordinance confers the powers and responsibilities of the "contracting government" upon the director of the Marine Department.[452] Accordingly, the director, or his/her designee, can set the Security Level, recognize security organizations to perform delegated functions, approve ship and facility security plans, audit and inspect ships and facilities, and issue security instructions to ships and facilities.

The legislation does not mandate that Part B of the code be implemented, but it does require company, ship, and facility security officers to "take into account the guidance contained in Part B of the code."[453] While the Marine Department is given ultimate

responsibility in the legislation to approve the plans and any amendments to them, the legislation does not specify the roles of other agencies and consultative bodies, such as the police department or the Port Facility Security Working Group.

The ordinance designates powers to "authorized officers," which include ranking Marine Department Inspectors, ranking police officers, and other public officers delegated by the director of the Marine Department. While these authorized officers are given authority to inspect ships and facilities, the legislation does not further delineate the roles of government agencies.

ISPS Roles at the Port

The Marine Department is Hong Kong's Designated Authority for implementation of ISPS. Hong Kong established three separate bodies to enact the Marine Department's implementation of ISPS, including the Administrative, Port; the Administrative, Ship; and the Operations Arm.[454]

> **Administrative, Port** - This body is responsible for the administration of all port security matters pertaining to ISPS. The PFSWG falls under this arm of the Marine Department. However, the PFSWG is more specifically designated as the executive arm of the Marine Department for ISPS implementation. [455]
>
> **Administrative, Ship** - This body is responsible for all matters pertaining to the security of vessels flying the flag of the HKSAR. [456] The Marine Department has authorized 8 different Recognized Security Organizations (RSO), per ISPS regulations, to "vet Ship Security Assessment, approve Ship Security Plans (SSP), conduct shipboard verification and issue International Ship Security Certificate (ISSC) to Hong Kong registered ships".[457]
>
> **Operations Arm** - This body is tasked with oversight of the day-to-day security measures, conducting drills and exercises, and coordinating the government's response to security issues. The Vessel Traffic Center, which provides 24-hour response for any maritime emergencies, is responsible for the duties of the Operations Arm.[458]

ISPS requires that all port facility operators create a Port Facility Security Assessment (PFSA). Once completed, these documents should be submitted to the PFSWG for evaluation.[*] If approved, the assessment is recommended to the Marine Department for its approval. All but one of Hong Kong's PFSAs were recommended for approval upon initial submission.[459] Once approved by the Marine Department, the facilities are required to create a Port Facility Security Plan (PFSP), which, in turn, must be submitted to the PFSWG for evaluation. Again, if acceptable, the PFSP is recommended to the Marine Department for approval. Once approved, the Marine Department issues a letter of compliance to the operator. All Hong Kong Container Terminal Operators

[*] October 2003 was set as the deadline by which all PFSAs had to be submitted to the PFSWG.

successfully achieved compliance before the July 2004 deadline.[460] Although river terminals are not international facilities and are not required to be ISPS compliant, many voluntarily adhere to the ISPS security guidelines.[461]

Per ISPS, the Designated Authority (Marine Department) sets all port security levels, upon the recommendation of the Police. ISPS security levels were developed by matching them to pre-existing terrorist threat levels used by the Hong Kong Police Force.[462] Per ISPS, the ability to respond to set security levels is key to both the ship and port facility security plans.[463] Since implementation of ISPS, the security level of the port of Hong Kong has remained low, at level 1.[464]

Customs Regime

The Hong Kong Customs and Excise Department (C&ED) was created through Article 116 of Hong Kong's Basic Law. [465] * This law permits Hong Kong to maintain a separate Customs structure from mainland China. The Department falls under the jurisdiction of the Secretary of Security, Mr. Ambrose Lee, and is chaired by Mr. Timothy Hong, Commissioner of Customs and Excise.[466]

The mission of the Hong Kong Customs and Excise Department is as follows:

- "To protect the Hong Kong Special Administrative Region against smuggling;
- To protect and collect revenue on dutiable goods;
- To detect and deter narcotics trafficking and abuse of narcotic drugs;
- To protect intellectual property rights;
- To protect consumer interests;
- To protect and facilitate legitimate trade and industry and to uphold Hong Kong's trading integrity; and
- To fulfill international obligations."[467]

The Customs and Excise Department is divided into five branches, each of which is headed by an Assistant Commissioner.[468] The Boundary and Ports Branch is charged with responsibility for the prevention of smuggling, Customs clearance for air/sea

---

* This article states: " The Hong Kong Special Administrative Region shall be a separate customs territory. The Hong Kong Special Administrative Region may, using the name "Hong Kong, China", participate in relevant international organizations and international trade agreements (including preferential trade arrangements), such as the General Agreement on Tariffs and Trade and arrangements regarding international trade in textiles. Export quotas, tariff preferences and other similar arrangements, which are obtained or made by the Hong Kong Special Administrative Region or which were obtained or made and remain valid, shall be enjoyed exclusively by the Region."

passengers and freight, search and seizure on any vessels in Hong Kong waters, and patrolling Hong Kong waters and coastline.[469]

Hong Kong is a free port and, as such, there are no tariffs or taxes on the import/export of goods.[470] * Customs clearance of imported goods is conducted through written inspection documents, such as manifests. When deemed necessary a physical inspection of goods and/or vessels is also conducted.[471]

As mentioned above, one of the primary duties of Customs and Excise is the prevention of smuggling. Customs works jointly with the Hong Kong Police, as well as multiple mainland China agencies to prevent narcotics smuggling. In an effort to prevent smuggling by sea, the Hong Kong government created the Joint Police/Customs Anti-Smuggling Task Force. C&ED maintains 24-hour maritime patrols of Hong Kong's territorial waters, and also maintains 6 launches to carry out any necessary interceptions at sea.[472] In similar fashion, the Control Points Investigation Division was created to prevent smuggling activities on land. In addition to inspections, the department "deploys drug detector dogs and introduces advanced technologies, such as Mobile X-ray Vehicle Scanning Systems and Vehicle X-ray Inspection Systems, to assist anti-narcotics work."[473]

Customs and Excise Participation in Multi-Lateral Initiatives

Hong Kong and China

As mentioned, Hong Kong and mainland China have distinct Customs agencies and legislation. Due to the increasing volume of trade between Hong Kong and the mainland, coordination of Customs and security procedures has become an increasingly salient issue for Hong Kong trade. Many complaints have been made that Chinese Customs procedures are opaque and often allow local officials too much leeway in enforcement of the law.[474] With its accession to the WTO, China has been moving to clarify and firmly enforce its Customs rulings.[475] As a part of this movement, Hong Kong and Shenzhen Customs have recently approved a joint "GreenLane" pilot project that will be unveiled in the coming months. The project will create an express lane across the Hong Kong-mainland border, allowing Customs procedures to be conducted at a logistics center in Shenzhen rather than at the border itself. OnePort Limited will provide a platform for the new "GreenLane" model that will facilitate the use of electronic data exchanges across the boundary. These data exchanges will include the "Unified Road Manifest for pre-submission via monitoring e-tools endorsed by Customs authorities."[476] If successfully implemented, the original "GreenLane" model will be expanded to the Shenzhen Western Corridor and Lok Ma Chau, thus providing coverage of all cross-boundary points.[477] In addition, the U.S.' Container Security Initiative was recently expanded to include the Port of Shenzhen in July 2005.[478] The addition of the CSI program in Shenzhen will further aid and strength Customs coordination between Hong Kong, the United States, and China.

---

* However, excise duties are charged on four goods: hydrocarbon oil, liquor, methyl alcohol, and tobacco.

APEC and the WCO Framework of Standards

As a member of both the WCO and APEC, Hong Kong fully supports the WCO's SAFE Framework of Standards to Secure and Facilitate Global Trade and the identical Framework for Secure Trade that was concurrently introduced by APEC. Some elements of the Frameworks are already being applied by Hong Kong Customs. However, C&ED is not yet ready to fully implement all elements of the Frameworks. Because neither organization has placed a firm deadline on implementation of the Frameworks, and as some elements need further elucidation, Hong Kong will take an incremental approach to implementation. Implementation will begin with those elements of the Frameworks for which Hong Kong is already well-prepared, including enforcement capabilities, use of radiation detection equipment, and joint targeting between Customs agencies. Some other elements of implementation will evolve over a longer time frame, as they may require passage of new legislation and/or significant changes for members of the supply chain.[479]

Customs and Excise Cooperation with Private Initiatives

Recently, several private terminal operators have worked to create technology that will facilitate easier and more secure Customs clearance procedures. Founded in 2003 by Hong Kong International Terminals, Modern Terminals Ltd., and COSCO-HIT Terminals, OnePort Limited aims to facilitate a secure, electronic information exchange between all port users. One of the key services offered by OnePort is its Advanced Customs Document Services. Through this service OnePort aims to assist "the shipping lines, NVOCC's and shippers in complying with the new U.S. Customs requirements to submit manifest data 24 hours prior to cargo loading through a low cost, easy to use and robust solution while protecting sensitive customer data."[480] In addition, OnePort anticipates being able to provide early notification of Customs inspection requests to participating carriers.[481]

Additional Considerations

One of the greatest difficulties of using global Customs agencies to increase port security is that not all Customs agencies were designed with the same purpose in mind. Traditionally, many Customs agencies, including Hong Kong, have focused on inbound cargo. The U.S. emphasis on pushing out borders through inspection of outbound cargo represents a fundamental shift in focus and practices.[482] U.S. government agencies should recognize the paradigmatic shift that programs such as CSI represent for many countries; such programs will require some time to be completely integrated. Accordingly, the U.S. government should facilitate the necessary dialogues and cooperation to bring about full standardization of practices among participants.

Lessons Learned and Conclusions

As the busiest container port in the world, the security of the Port of Hong Kong is fundamentally important for the U.S. U.S.-China trade is steadily increasing, and the majority of this trade passes through Hong Kong.

Hong Kong has implemented some of the most sophisticated port technology in the world. Security practices are not so much driven by fears of local or regional terrorism as by economic concerns. There is little concern that Hong Kong itself will be a target of terrorism. However, there is great concern that a worldwide terrorist incident could shut down the flow of traffic in and out of the port. Hong Kong businesses and officials realize that the economic survival of their city depends on international perceptions of Hong Kong as a secure shipment hub. Hong Kong also recognizes that it faces increasing competition from mainland China ports, and that its ability to provide more secure facilities will continue to give it a necessary edge over Chinese ports. The most significant security initiatives in Hong Kong thus far have been prompted by the private sector. In recognition of the interdependence of global trade, Hong Kong's terminal operators have been some of the biggest advocates of security for the entire supply chain, and not just port facilities alone.

The terminal operators at the Port of Hong Kong are some of the largest port operators in the world; as such, they are leaders in the drive for global supply-chain security. Initiatives such as ICIS and the Smart and Secure Tradelanes, implemented by many of the Hong Kong operators are forward-thinking, multi-national initiatives. They represent attempts to secure not only port facilities, but the entire supply chain itself. Such efforts should be increasingly acknowledged as necessary for global security. Port security is only one element of cargo and trade security, and such initiatives recognize this.

Although the private sector has implemented very advanced security practices, the government of Hong Kong needs to take a more proactive role in this process. As a business-minded city, the Hong Kong government has tended to take a minimalist approach to regulations and procedures. However, such an approach limits not only intra-governmental relations, but also procedures between the Hong Kong government and private agencies. One of the greatest weaknesses of the ICIS project is the lack of government participation. To date, should the private terminals discover a security threat during the screening process, there are no standardized protocols for government response. The capabilities of the ICIS technology will be wasted unless the Hong Kong government and other governments work together to create best-practices procedures to respond to threats.

Additionally, one of the greatest difficulties for Hong Kong security at the moment is the increasing volume of trade flowing back and forth from China. Hong Kong Customs and security can only be as strong as Chinese procedures; tales of falsified Chinese Customs documents and lax Chinese officials abound. Additionally, the increasing volume of trade between China and Hong Kong makes clear the increased importance of Hong Kong's mid-stream terminals. However, because these terminals are not required to be ISPS compliant, an increasing portion of Hong Kong's trade flows through terminals that are not subject to any international standards. The lower security standards for mid-stream terminals and the lack of unified Customs procedures between China and Hong Kong make clear that without increased standardization, Hong Kong's security will be significantly weakened. Such standardization cannot be expected to

come through the private sector, the Hong Kong and Chinese governments must work together to implement stronger initiatives in this area.

Lack of government cooperation will be the biggest difficulty not only for the security of Hong Kong, but also for the world as a whole in the coming years. The benefits of secure trade are macroeconomic, and similarly, the costs of a security incident would be borne by all. However, thus far, the costs of security and supply chain initiatives have primarily fallen on the private sector. Governments must work to make the costs of security as widespread as the benefits. Additionally, security initiatives such as the ICIS project represent a step forward in security capabilities, yet governments have been slow to embrace such private efforts. If private companies are expected to continue to seek security innovations, governments must provide increased incentives to do so. Intra-governmental cooperation must be increased if international security initiatives are to be successful. True global trade security will require visibility of the entire supply chain, and coordination amongst all involved parties and countries.

Chapter 8. India and the Port of Jawaharlal Nehru

Introduction

India is located in Southern Asia, bordering the Arabian Sea and the Bay of Bengal, between Burma and Pakistan. Its total geographic area is 3,287,590 sq km, with a population of 1,080,264,388 people (2005 est.). India's populace comprises several religious groups: Hindus, 80.5%; Muslims, 13.4%; Christians, 2.3%; Sikhs, 1.9%; and others, 1.8% (2001 census). It is important to note that 25% of India's population, roughly 250 million people, lives below the poverty line. Yet, the country has quickly become a force in the global economy, with an estimated 2005 Gross Domestic Product of US$3.7 trillion.* India is also a vital participant in international trade. In 2005, exports amounted to $76.2 billion, and imports totaled $113.1 billion. Of this trade, 17% of exports were destined for the United States, and 6% of imports originated in the U.S. India has 63,230 km of railways, 3,851,440 km of roadways, 14,500 km of waterways, and 7,000 km of coastline. India's major ports and inland terminals include Chennai, Haldia, Jawaharlal Nehru, Kandla, Kolkata (Calcutta), Mumbai (Bombay), New Mangalore, and Vishakhapatnam.[483]

National Structures

Port Administration/Authority

Over the course of the last 40 years, India has slowly decentralized its authority over port administration through legislative acts that have created autonomous bodies and legal authorities.

Ministry of Shipping, Road Transport and Highways

Federal authority for India's port administration falls under the Ministry of Shipping, Road Transport, and Highways. This Ministry was created on February 9, 2004, through the merger of the Ministry of Shipping and the Ministry of Road Transport.[484] Within this ministry, the Department of Shipping is responsible for India's ports, national waterways and inland water transport. The Department is also responsible for the formulation of maritime policies and programs and their implementation. According to the Indian Constitution, the Department of Shipping has jurisdiction over the administration of the Indian Ports Act of 1908, and the Major Port Trusts Act of 1963 (MPTA).[485]

Major Port Trusts

As part of a larger decentralization effort, the MPTA provided for the creation of a Port Trust at each of India's major ports and vested the central administration, control and

* Unless otherwise noted, all currency is listed in U.S. dollars.

management of these ports in their respective Port Trusts. India's minor ports fall under the administration of their respective state governments. At present, India has 12 major ports, and approximately 180 minor ports. The 12 major ports included in the MPTA are Kolkata, Mumbai, Chennai, Kochi, Kandla, Vishakhapatnam, Paradip, Tuticorin, New Mangalore, Marmugao, Jawaharlal Nehru and Haldia Dock.[486]

The primary functions of the Major Port Trusts (MPTs) are to raise capital and maintain economically efficient and secure operations that will facilitate India's economic growth. Since the enactment of the MPTA, India has established 11 MPTs.[487] The Port of Ennore, the only major port not run by an MPT, is designated as a corporation under the authority of the Central Government.[488]

The authority for each MPT is embedded in a Board of Trustees. Following the MPTA, the Central Government transferred all port assets and liabilities to the Boards, and declared all future obligations and contracts to be each Board's responsibility. The Central Government still maintains some control over MPTs by appointing the Chairman of the Board of Trustees and maintaining the authority to appoint additional officers. The MPTA states that the Board must include representation from port employees, the Mercantile Marine Department, the Customs Department, its respective state government, the Defense Services, the Indian Railways and any other interests that the Central Government believes should be represented on the Board. [489]

The Tariff Authority for Major Ports

In order for the Central Government to balance the expansion of market-based reforms within a centralized framework, the Central Government established the Tariff Authority for Major Ports (TAMP) through the Ports Laws (Amendment) Act of 1997. [490] The TAMP serves as an independent authority to regulate all tariffs, both vessel related and cargo related, within the major ports. This body is also responsible for regulating the rates at which ports may lease facilities and provide services. Although the TAMP fixes tariff ceilings for services rendered by major ports, the ports are permitted to fix tariffs at any level below the aforementioned ceilings.[491] The TAMP is composed of a chairperson and two additional members, all appointed by the Central Government. This Authority has jurisdiction only over the 12 major ports and the private terminals within these ports.

Private-Sector Operators

Prior to the passage of the MPTA, most port investments were made by the Central Government. However, increasing resource requirements and efficiency concerns have recently led to the active involvement of the private sector in infrastructure development.[492] To encourage private participation, the Department of Shipping has created comprehensive policy guidelines for private-sector participation at the ports.[493] MPTs are now permitted to lease out their existing assets to private entities and/or to contract with private developers for the construction of new assets such as container terminals, cargo berths, and warehouse facilities.[494] In addition, MPTs are allowed to

lease out 100% captive facilities (including oil jetties, platforms etc.) to port-based industries.

Thus far, most private-sector lease agreements have been in the form of *Build-Operate-Transfer (B-O-T)* schemes. Under B-O-T arrangements, private operators are chosen from tenders collected through open bidding processes, at which point, the winning operator takes over the development and management of port facilities for a specified lease period. However, the MPTA mandates that the Central Government retains the right of ownership over port land. Lease arrangements may be no longer than thirty years, at the end of which, assets will revert back to the port.[495]

National Port Security

In an effort to balance federal and state powers, India's constitution delineates separate national and state responsibilities for port security. Individual states are responsible for public order and policing within their local jurisdictions, while the central government's responsibilities are to protect ports from interstate or international conflict and to maintain the free flow of trade.[496] According to the MPTA, Major Port Trusts fall under national jurisdiction. The following are national agencies with special responsibilities for port security.

Ministry of Home Affairs

The Ministry of Home Affairs is responsible for all matters relating to internal security, as well as all matters relating to intra-state and inter-state relations.[497] Within the Ministry of Home Affairs, the main agencies responsible for port security are the Central Industrial Security Force and the National Security Guards, India's counter-terrorism force.

Central Industrial Security Force

The Central Industrial Security Force (CISF) was established through the Central Industrial Security Force Act of 1968.[498] In 1983, the CISF was made an Armed Force of the Union.[499] Through subsequent legislation and mandates, the CISF has evolved into one of India's most important security agencies. Today, it is the largest paramilitary force in the nation with over 93,000 personnel. CISF specialists are trained in intelligence gathering, fire prevention, internal security and disaster management. Some members have specialized training in rescue and relief operations for major calamities, including nuclear, biological and chemical emergency response. At present, the CISF provides security for a myriad of facilities, including airports, seaports, MPTs, hydro-electric projects, space installations and nuclear plants. [500]

The main role of the Central Industrial Security Force is to protect India's Industrial Undertakings.[501] To help reduce corruption, CISF employees are generally rotated through multiple industries during their careers. Indian law defines an "Industrial Undertaking" as any entity engaged in industry, trade, or services that may be regulated by Parliament.[502] The government passed a law stating that all such institutions are required to employ the CISF for security. Given this new responsibility, the CISF has

grown rapidly in recent years. A 1999 amendment to the CISF Act further expanded the CISF's scope of work by enabling it to provide consulting services to private sector establishments.[503] The CISF also retains the legal right to conduct searches without a warrant. [504] Despite the CISF's growing power and authority, it is still required to coordinate with state and local authorities.[505]

Numerous complaints have arisen regarding the expansion of the CISF's powers. Reports have accused the Force of engaging in official corruption and human rights abuses.[506] In 1996, the Madras Port Trust board approved a plan for disbanding the CISF at its port, and creating its own security force.[507] In spite of complaints against it, the CISF remains the largest and most influential central paramilitary force in India.

National Security Guards

The National Security Guards (NSG) is a federal contingency deployment force that tackles all facets of terrorism in the country. Its primary role is to engage and neutralize terrorist threats in specific situations. The NSG is composed of 7,330 troops trained in counter-hijack operations involving piracy in the air, land and water. It maintains a national Bomb Data Center and conducts bomb disposal and post-blast investigations. The NSG also trains the Armed Forces and State Police in special commando bomb disposal and security. The NSG was modeled after the United Kingdom's SAS and Germany's GSG-9 security forces.[508]

Customs Regime

Organization

The Central Board of Excise and Customs (CBEC) is a part of the Department of Revenue under the Ministry of Finance. The Board is responsible for the formulation of all policies concerning levies, central excise duties and smuggling prevention. In addition, the Board administers all matters relating to Customs Houses, Central Excise, and Narcotics.[509] The CBEC's current regulatory authority and responsibilities were established through the Indian Customs Act of 1962. Although the Board has a variety of security powers, its main focus is on revenue collection and facilitation of trade.

Primary Strategies

The CBEC is currently employing several specific strategies to achieve its objectives. Many of these strategies and objectives are similar to those espoused by the U.S. Customs and Border Protection.[510]

Enhancing the Use of Information Technology – The CBEC seeks to promote electronic commerce and expedite cargo clearance through the use of automated import/export processes and an Electronic Data Interchange.

Streamlining Customs and Excise Procedures – The CBEC is placing an increased focus on advanced risk assessments and reduced human intervention.

Encouraging Voluntary Compliance – The CBEC hopes to encourage private-sector compliance by consulting with concerned trade interests before introducing legislative changes.

Evolving Cooperative Initiatives – The CBEC is trying to foster interagency initiatives within India, as well as participation in international initiatives led by organizations such as the World Customs Organization and the World Trade Organization.

Combating Revenue Evasion, Commercial Fraud and Social Menace -The CBEC hopes to make better use of intelligence systems and emerging technologies through the use of information analysis, strategic threat assessment, and a professional audit system.

Special Security Provisions

Among the various responsibilities assigned to the CBEC, the following pertain directly to its role in national security:[511]

- Maintenance of the security of India;
- Prevention of smuggling;
- Protection of human, animal or plant life or health;
- Fulfillment of obligations under the Charter of the United Nations for the maintenance of international peace and security; and
- Implementation of any treaty, agreement or convention with any country.

Although the CBEC focuses more directly on revenue collection than security, the Customs Act does provide the Board with several security powers. These include the power to arrest, to inspect, to search, and to use force. A more complete list of the CBEC's special security powers is provided in Appendix 8a.

Port Case Study - Jawaharlal Nehru

General Port Information

Jawaharlal Nehru is situated along the eastern shore of Mumbai harbour, southeast of Elephanta Island. The port was originally built as a satellite facility, in an effort to decongest traffic at the Port of Mumbai. However, Jawaharlal Nehru quickly became India's busiest container port, handling over 60% of the country's container cargo by the end of 2003.[512] The port also houses modern facilities for handling dry-bulk cargo, with a designed capacity of 3,500,000 tons in the bulk terminal. Although the port was initially planned and constructed for handling dry-bulk and containerized cargo, port facilities have been upgraded for handling vehicles, iron ore and liquid-bulk cargoes.

Jawaharlal Nehru Port is an all-weather tidal port and is the only Indian port built to international standards, with high levels of automation and computerized processes.[513]

Cargo volume is rapidly increasing at the Port of Jawaharlal Nehru. In 2005, the port handled 36.21 million tons of cargo (container, liquid-bulk, break-bulk and vehicle). Container traffic accounted for 2.58 million TEUs of this total cargo volume, a 9.32% increase over the previous calendar year.[514] Container traffic has been growing rapidly in recent years, with annual growth rates of approximately 25%. In contrast, bulk cargo has been steadily declining. As a result, the Port Trust recently decided to convert its bulk terminal into a container terminal.[515] With the addition of this new terminal, the port is expected to add 1.3 million TEUs of annual container capacity.[516]

Stakeholders

Jawaharlal Nehru Port Trust (JNPT) Container Terminal

As one of India's 12 Major Ports, Jawaharlal Nehru comes under the authority and ownership of a Major Port Trust. The Jawaharlal Nehru Port Trust (JNPT) is the most recently established MPT in the country, having been commissioned on May 26, 1989. Aside from its ownership of the port, the JNPT also operates one of the port's two container terminals.

The JNPT Container Terminal includes three berths with a linear quay length of 680 meters, a main container yard spanning 35 hectares (30,000 TEUs capacity) and an additional paved area of 180,000 sq meters.[517] The terminal has a container capacity of 1.3 million TEUs per annum, and is capable of handling third generation container vessels.

Nhava Sheva International Container Terminal (NSICT)

NSICT is India's first privately managed container terminal and the first entirely automated container terminal to be developed in India.[518] The terminal is operated by P&O Ports, a subsidiary of the Peninsular and Oriental Steam Navigation Company, which was recently bought by Dubai Ports World.[519] Developed at a cost of $250 million, the NSICT started operations in April 1999, and is managed under a Build-Operate-Transfer agreement between P&O Ports and JNPT. The terminal has a capacity of 1.3 million TEUs per annum and is capable of handling fifth generation vessels.[520]

Terminal responsibilities are shared by JNPT and P&O Ports. JNPT is responsible for scheduling entry and berthing of vessels, pilotage and towage, dredging and maintaining navigational safety. P&O Ports, on the other hand, is responsible for the operation, maintenance and repair of all port equipment.[521]

Liquid-Cargo Jetty

In August 1999, the JNPT granted a B-O-T lease to Bharat Petroleum Corporation Limited and Indian Oil Corporation Limited for the construction of a twin-berth, liquid-

cargo jetty. The cargo jetty has been functional since March 2002 and can accommodate ships at a seaside or shore side berth.[522]

Port Security

Law Enforcement

As previously described, the Central Industrial Security Force is the primary security presence at all of India's ports. Local law enforcement is present at the port, but does not play an integral role in security affairs. However, any security incidents that require an arrest must be handled by the Mumbai police.[523]

According to Indian law, all port law enforcement bodies work independently and report to the Chairman of the Port Trust, as well as to the Ministry of Home Affairs. CISF reports to the JNPT administration, as well as to the Deputy Port Facility Security Officer.

Physical Security

The Port of Jawaharlal Nehru has only one vehicular entrance that is manned by guards 24 hours, 7 days a week. There is only one land-side entry and exit point and all entering persons must pass through metal detectors. The entire port premises are fenced with both land-side and water-side entries protected 24 hours per day by armed CISF guards. Additionally, Customs employs two scanning machines (one x-ray and one gamma ray) that may be used on cargo.[524]

JNPT maintains a central administration building that is responsible for all port facilities, but lacks a central command tower with a visible view of the entire port. Instead, CISF deploys security agents at various strategic checkpoints throughout the port facilities.[525] The NSICT terminal, however, has a central command tower for its own facilities that can communicate with JNPT via radio.

NSICT has instituted multiple security upgrades that are superior to the overall port security. The terminal installed a lighting system to cover its entire fence-line, container storage facilities and docking areas. An exterior camera system monitors the terminal from two separate towers as well as the access gate, while interior cameras observe every floor of the NSICT building. NSICT's private security personnel monitor the camera system.[526]

Although the JNPT-operated terminal has cameras at its entrance gates, as of yet, these cameras have not been installed. JNPT plans to install these cameras within six months, as well a CCTV system that will be monitored 24 hours per day.[527]

Restricting Access and Background Checks

Photo ID passes are one of the primary methods used to restrict access at Jawaharlal Nehru. Any worker or visitor at the port must have a photo ID pass, unless accompanied by an escort from the JNPT administration. Prior to receiving an employee photo ID,

workers must be verified and approved by JNPT. To receive verification, employees must pass criminal checks with both local and state police, as well as national security checks through the CISF.[528] At the NSICT terminal, P&O Ports conducts its own additional private background check on all employees and visitors entering its facilities.[529] Building and terminal access is also restricted through biometric finger scans. All port employees and over 600 contractors are registered in the biometric system.

In order to obtain a visitor pass, one must have business with the port that is cleared through a local import or export agent. The local agent applies to the port on behalf of the visitor, who must be cleared through a CISF background check. This process may take anywhere from a week to a month to complete. It is possible to obtain a quick pass to the port only if the visitor is escorted by port personnel at all times.

Entering cargo trucks are identified using a form that contains the driver's photo and license number and describes the number, content, and destination of all containers in the vehicle. It is the responsibility of the shipping agent to complete this form and have it at the gate prior to the arrival of the truck. Truck drivers carry 3 copies of this form: one is given to Customs, one is given to CISF at the gate, and one is retained by the driver. Once inside either terminal, truck drivers are not permitted to leave their vehicles at any time.[530] In addition, all containers entering or exiting the port's two container gates must have a locked seal. CISF guards provide armed protection at all times for both container gates and check the seals on every entering/exiting container.[531] At NSICT, if any seals are found to be broken or damaged, Customs is immediately notified. NSICT officials noted that JNPT does not run the "same" system for checking seals, and might not report all discrepancies.[532]

Once again, NSICT has instituted additional measures to restrict access at its terminal. NSICT operates a tracking system called NAVIS, which allows operators to track containers and trucks via Radio Frequency Identification. The NAVIS system, developed in Oakland, California, can track every container in real time, detailing when, where, and by whom a container is moved. At NSICT, every truck is logged in to the NAVIS system upon entrance, and no truck is allowed to remain in the terminal for longer than one hour.[533] NAVIS data are also used to provide cargo information to shipping lines.[534] Although JNPT has purchased the NAVIS system and plans to implement it, it is not yet equipped to do so.[535]

Security Personnel and Training Requirements

At the JNPT terminal, 400 CISF guards operate on 8-hour shifts, conducting between six and twelve patrol rounds per day. Guards patrol both outside and within the terminal area, using jeeps, motorcycles and bicycles.[536] All CISF guards are former military officers who also receive training in fire prevention, emergency medical treatment, paramilitary operations and ISPS code compliance. Operators at both terminals reported that CISF training requirements are extremely stringent, even by military standards.[537] To reduce potential for corruption, CISF guards remain at the port for only 3 years before being transferred elsewhere.[538]

At the NSICT terminal, 25 to 30 CISF guards patrol the premises at any given time. In addition, NSICT has hired its own private security force to patrol the terminal. In 2003, the terminal contracted with a company called Checkmate, based out of Mumbai. Checkmate is a private security force comprising veteran military officers with specialized training. Employees receive additional training in first aid, firefighting, and basic ISPS code compliance. Checkmate guards overlap with CISF patrols, consistently providing an additional five to ten guards NCIST's private security is primarily used as a "watch and ward" detail to provide vigilance rather than paramilitary engagement.[539]

Exercises and Drills

The JNPT emergency security team runs joint drills that involve all local police officers stationed at the port, the Indian Army, the Navy, and the Air Force. Once a drill has concluded, JNPT conducts a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis to evaluate the port's performance. If a security weakness is identified as a result of a drill exercise, it is immediately addressed. According to Captain Jitendra Mishra, Deputy Conservator of JNPT, the port implements the necessary solutions, and then, "in the next security exercise, we [SIC] put more emphasis on the identified weakness to see whether our solution is favorable." [540]

NSICT is included in the port's joint-security plan and its overall security is the responsibility of JNPT. However, NSICT conducts its own security planning and employs a Chief Warden to oversee its security operations and exercises. Once a month, NSICT conducts drills with its own Emergency Team, which consists of the engineering, fire, hazardous material and operations departments at the terminal. All monthly drills are filmed and reviewed, and once every quarter, the terminal also conducts joint exercises with CISF and JNPT. NSICT drills frequently simulate fire, water and industrial accidents that might occur at the terminal, or within a container shipment. Many exercises are tabletop exercises that involve the Air Force, Navy and local police; the terminal also conducted two live exercises in the last year.[541]

Suggestions for Improving Security

Most of the suggestions for improvement made at the JNPT terminal revolved around intelligence issues. Officials believe that improvements to national and international intelligence services are the key factors needed to enhance port security. Captain Mishra did note, however, that JNPT would also like to implement a camera system along the fence-line and link it to a centralized CCTV system.[542]

In contrast, officials at NSICT suggested that better technology and access to information would most improve their security operations. NSICT officials would like more timely access to vessel departure and arrival information, and expressed a certain frustration with the process used by JNPT and Customs to disseminate ship and cargo information. Specifically, Mr. Sujeet Singh, General Manager of Operations, noted that NSICT would like to receive information about any vessel bound for its terminal either before or at the time the vessel departs its port of origin. Officials also expressed a desire to obtain information regarding export containers more than 6 hours in advance. Mr.

Singh acknowledged that although better access to and analysis of cargo information would improve security, current technological limitations hinder this process. Finally, NSICT officials mentioned that they would like to obtain electronic container seals with centralized receivers.[543]

ISPS at the Port of Jawaharlal Nehru

The Indian Government mandates that both the compulsory Part A and the voluntary Part B of ISPS must be implemented at Indian ports. Officials at both Jawaharlal terminals reported 100% compliance with both parts of the Code and neither terminal reported any difficulties with the definition of ISPS compliance. None of the officials interviewed saw any deficiencies with the Code or had suggestions for improvement.[544]

The primary benefit JNPT officials believe ISPS implementation has brought to Jawaharlal Nehru is an increased awareness of security issues. Captain Mishra expressed a firm belief that security is aided far more by human intelligence than equipment or technology. Mishra noted an increased awareness not only among port employees, but also in other port users, the shipping circle and shipping agents. He believes this awareness has helped because, "odd behavior is more easily noticed and now it is reported to the right people. The more awareness that comes from people on the ground, the easier it is to secure the premises." [545]

Officials at NSICT noted additional improvements brought about by ISPS implementation. Captain Girish J. Munjal believes ISPS has allowed for more cooperation, interaction and a clearer definition of individual roles at the port. He stated, "each person understands what they are supposed to do … there is a better understanding of what role government agencies can provide, what resources they have, and who should be responsible." [546]

Customs at the Port of Jawaharlal Nehru

Interface with Stakeholders

In its continuing efforts to facilitate trade and excise through collaborative technology, Customs has created an Electronic Data Interchange that links all port stakeholders, including importers/exporters, the JNPT administration, and various government ministries, through a single network. Customs communicates electronically with the port through a system exchange of messages (SMS), which allows independent agencies to maintain separate databases and proprietary information while communicating through a pre-defined protocol.[547]

Although Indian Customs places great emphasis on the use of technology, many importers do not currently have the necessary technology to file their documents electronically. When importers are unable to file electronically, they must bring their paper documents to the Customs onsite service station, where documents are then manually entered into the system. If an importer cannot go to the service station, paper documents or a floppy disk must be mailed to the Customs office. Currently, over 40% of manifests are filed electronically, and that percentage is rapidly growing. However,

the inability of many import companies to comply with the necessary electronic procedures is troublesome, and will become increasingly so, as Customs intends to close down the onsite service center within the next two years. [548]

Types of Inspections

Indian Customs subjects 100% of entering goods to a thorough assessment process, during which it examines import documents, bills of lading and the vessel manifest. Customs also employs an advanced targeting system that determines which consignments may need further assessment or examination.[549] The targeting system pinpoints goods for physical inspection based on the nature of the good, the port of origin, the importer and the shipping line. At present, 70 to 80% of all consignments are physically examined. Certain clients with a proven history of compliance and honesty can receive an "accreditation," which allows them to enjoy a greatly simplified assessment process and to avoid physical examinations. [550]

In addition to physical inspections, Customs also uses two scanning machines to examine cargo. One of the machines is a mobile x-ray machine that moves between terminals, while the other, a gamma-ray machine, is stationed in the Container Storage Facility outside the terminal area. Customs scans roughly 5 to 8% of all entering containers, which amounts to approximately 200-300 container scans on a daily basis. In order to decide which containers will be scanned, Customs uses a software profiling system that looks for suspicious documentation. The profiling system analyzes information in the import manifest and the bill of lading. When the software identifies and selects a suspicious container, it automatically notifies the shipping line that a container has been selected for scanning. The mobile x-ray machine is used as a first-level scanner in order to gather information before the consignment is scanned at the Container Storage Facility by the gamma-ray machine. After examining the scanned images, Customs agents will then decide what level of physical examination is required for the goods in question.[551]

Best Practices (New Risk Management System)

Jawaharlal Nehru Custom House is the first port to implement India's new risk management system software. This software was previously implemented at both the Mumbai and New Delhi airports, but JNPT is the first port to implement the system for Maritime Customs. JNPT began a phased implementation in February 2006.

The software program conducts a real-time information analysis of documentation provided through the Customs Electronic Data Interchange. The program conducts an automated risk assessment of cargo information and provides decisions to Customs officials at the port. Additionally, the software includes a feedback process that provides Customs officers with analysis and advice on appropriate actions. Any documents belonging to a single import/export company are analyzed jointly and linked to the company's history, thus allowing Customs to more easily identify suspicious companies. The main advantages of this system are: 1) it provides Customs officials with easier

access to more complete information; and 2) by automating the decision-making process, risk assessments are more uniform. [552]

Types of Advance Information Required for Vessel/Cargo Clearance

Customs requires cargo information in the import manifest to be submitted prior to arrival at the port. Cargo information is then combined with vessel information to run a security profile.[553] Vessel agents must obtain a Vessel Identification Advise (VIA), two or three days prior to arrival. The JNPT Operations Department uses this document to make sure the vessel is cleared through all appropriate departments.[554] Ships must also submit arrival information at least 48 hours prior to reaching the port. This information should include the vessel's name and master, port of registry, last port of call and any classes of dangerous cargoes. [555]

CSI

Although Jawaharlal Nehru has signed an agreement to implement CSI, the program has yet to be put into practice. The Indian government remains enthusiastic about CSI and plans to implement the program in the near future. Joint Commissioner S.A. Usmani noted, "India's security concerns are directly related to U.S. security concerns. Without help from external sources of intelligence, India will not be able to enhance its own intelligence." [556] Indian Customs agents believe CSI will fit well within their current operations, as they already inspect 100% of outbound containers. Customs agents are also interested in the reciprocal nature of the program.

The government's only source of concern about CSI involves unclear provisions for no-load orders. At present, the Indian government feels the CSI program does not clearly delineate the stages of the shipping process at which the U.S. may intervene to stop an export container. Indian officials are concerned that excessive no-load orders could negatively affect their shipping industry, and would prefer for this order to be used only in extreme circumstances. Additionally, the government remains unclear as to whether the Indian government or the U.S. government would bear the cost of this decision.[557]

Lessons Learned and Conclusions

Over the last thirty years, India has undergone one of the most notable economic transformations of the twentieth century. The country has purposefully and steadily moved away from its previous status as an isolated, import-substitution economy towards its current position as a leading participant in global trade. A vital component of the Indian government's modernization strategy is the emphasis it has placed on utilizing information technology to streamline processes and remove bureaucratic obstacles. India's technological advances have allowed the country to implement forward-thinking bureaucratic procedures, such as the Customs Electronic Data Interchange, which allow the country to more easily comply with rapidly advancing international security standards. Technological innovation has also made possible the construction of such advanced port facilities as Jawaharlal Nehru's fully automated NSICT terminal.

However, a full technological transformation of India's port facilities and procedures has yet to be realized. Many of India's port facilities lag years behind the technological prowess of the NSICT terminal, and although Indian Customs' electronic procedures are promising, the lack of a more uniform national technological infrastructure prevents many importers from being able to participate in the new system. Such large discrepancies in technological capabilities remain a notable impediment to India's economic and national security goals.

The broad spectrum of India's port security capabilities is especially apparent at the port level in Jawaharlal Nehru. The observed differences between the privately-operated terminal, NSICT, and the publicly operated terminal, JNPT Container Terminal, are startling. The private terminal far surpasses the public one in multiple areas, from the quality of its equipment, buildings and personnel, to the quality control of its processes. It remains unclear whether this difference is a due to better access to monetary resources or as a result of more efficient implementation and management. Yet, the superiority of the private terminal can be seen in its performance results. Despite its smaller size, NSICT has consistently outperformed all other Indian container terminals. As a result, JNPT is now soliciting private offers on a B-O-T basis for its new container terminal.

As India continues its modernization process, it is likely that more terminals will convert to private management. Such a change bodes well for the implementation of more advanced security procedures, as private companies are frequently able to harness resources more easily than fiscally constrained government agencies. However, this change will also require continued efforts to facilitate smooth communication between the private and public entities involved in port security. Lack of communication and information was one of the biggest complaints at the NSICT terminal. India is not unique in this regard: public-private cooperation appears to be one of the most difficult hurdles for many countries to overcome in order to obtain true supply-chain security.

Overall, India appears to be allying itself with the U.S. in both its foreign policy and national security goals. International security procedures such as ISPS and CSI have been well-received in India, and it is likely that the country will remain eager to participate in such initiatives. However, given the very different stage of India's economic development, the U.S. will need to clearly demonstrate to the Indian government that programs such as CSI will not hinder the free flow of trade. At the time of the port visit, most of the officials interviewed were more interested in revenue collection and facilitation of trade than protection against terrorism. The recent train bombing in Mumbai serves as a reminder, however, that India has frequently been the recipient of terrorist acts. It remains to be seen how greatly opinions will be changed by the Mumbai bombing, but it seems likely that these events will galvanize support for the implementation of international security initiatives and increased national security measures.

Appendix 8a

CBEC Customs Powers and Provisions[558]

Power to Inspect

A proper officer authorized by the Commissioner of Customs may enter any place or conveyance and inspect the goods stored within.

Power to Examine Persons and Produce Documents

During the course of a smuggling inquiry, a Customs officer may: 1) require any individual to produce documents or objects relevant to the inquiry and 2) examine any person acquainted with the facts and circumstances of the case.

Power to Search Persons

In order to conduct a search, the individual in question must be taken before a gazetted Customs officer and witnesses must be present to observe the search procedures.

Power to Summon Persons to Give Evidence

Any Customs officer has the power to summon individuals to produce evidence involved in a smuggling inquiry.

Seizure of Goods, Documents and Objects

If an officer has reason to believe that any goods are subject to confiscation under the Act of 1962, such goods may be immediately seized.

Customs Power to Arrest

If an officer has reason to believe that any person within India or its territorial waters has committed an offense, the officer may arrest such person.

Customs Officer has Same Powers as Police

When a Customs officer makes an arrest, the Code of Criminal Procedure provides this officer with the same powers and subjects him to the same provisions as any police officer.

Power to Stop and Search Conveyances

If an officer has reason to suspect the presence of smuggled goods, the officer may at any time stop any such vehicle, animal or vessel or, in the case of an aircraft, compel it to land, and

- rummage and search any part of the aircraft, vehicle or vessel;

- examine and search any goods in the aircraft, vehicle or vessel or on the animal;

- break open the lock of any door or package, if the keys are withheld.

Extra Measures/Use of Force

If it becomes necessary to stop a vessel or compel an aircraft to land, any vessel in the service of the Government, while flying India's proper flag, should first summon the vessel to stop by means of an international signal, code or other recognized means. If the summoned vessel fails to stop, chase may be given; if, after a gun is fired as a signal, the vessel still fails to stop, it may be fired upon. Should it become necessary to stop any vehicle or animal, the proper officer may use all lawful means for stopping it, and where such means fail, the vehicle or animal may be fired upon.

Chapter 9. Mexico and the Port of Veracruz

Introduction

Mexico is located in Middle America between the Gulf of Mexico and the Pacific Ocean. Occupying 1,972,550 sq km of geographic area, Mexico shares a border with the United States to the north and borders Belize and Guatemala to the South. In 2005, Mexico's estimated population was 107,449,525 people, approximately 40% of whom were living below the poverty line. As a participant in the tri-lateral North American Free Trade Agreement (NAFTA) with the U.S. and Canada, Mexico is one of the U.S.' primary trade partners. In 2005, 87% of Mexico's US$213.7 billion* in exports were destined for the U.S. Imports in the same year totaled $223.7 billion, of which 55.1% originated in the U.S. Mexico has 17,634 km of railways, 6,979 km of highways, and 2900 km of waterways.[559] The primary ports in Mexico are Altamira, Manzanillo, Lazaro Cardenas, Salina Cruz, Tampico, Topolobampo, and Veracruz.

National Structures

Port Administration (*Asociación Portuaria Integral - API)*

Mexican ports benefit greatly from their proximity to the U.S. and thus experience low relative transport costs when compared with the majority of other global ports.[560] In 1993, Mexico began a process of port privatization aimed at increased port efficiency and reductions in relative transport costs. By 1995, the Mexican government had granted concessions to private companies in Manzanillo, Ensenada, Altamira, and Veracruz. The ports adopted a landlord model, still used today, whereby the Mexican government maintains regulatory duties and ownership of the land but allows for private management of and financial responsibility for port terminals and equipment.[561]

Secretariat of Communications and Transportation *(Secretaria de Comunicaciónes y Transportes - SCT)*

The federal authority charged with administration of Mexican ports is the Secretariat of Communications and Transportation (*Secretaria de Comunicaciónes y Transportes - SCT*) based in Mexico City. The agency's primary mission is to facilitate and promote a high standard of transportation infrastructure development in Mexico in order to stimulate the economy and connect the nation with the rest of the world.[562] The SCT is responsible for major port administration decisions such as whether or not to take part in global partnerships like ISPS or CSI. In 2004, the agency operated with a budget of $2.8 million, more than two-thirds of which was provided to individual port authorities for infrastructure improvements and investments in the consumption of more sustainable energy.[563] Additionally, the SCT serves as the primary decision-making body in the event of port security incidents at all Mexican ports. Port administration falls to the SCT's division of "General Coordination of Ports and Merchant Marines."[564] Within

* Unless otherwise noted, all currency is listed in U.S. dollars.

this division exists a branch called the Ministry of Nautical Education, or FIDENA (*Fideicomiso de Formación y Capacitación Para el Personal de la Marina Mercante Nacional*), responsible for assessing ISPS compliance at all Mexican ports. The SCT's 2005 annual report outlined 48 goals and strategies for the near future, in which it expressed a desire to participate more consistently in international partnerships to secure cargo and facilitate more efficient trade relationships.[565]

All Mexican Ports recently adopted ISPS, known in Spanish as the PBIP (*Código de Protección para Buques e Instalaciones Portuarias*).[566] FIDENA, along with the board members of an international group of standards, annually assesses each port's compliance with global security initiatives.[567] Additionally, FIDENA is responsible for ISPS training programs in Mexico City and in four major nautical education schools located in Veracruz, Mazatlán, Tampico, and Campeche.[568]

National Maritime Legislation

In addition to ISPS, Mexico has adopted the Convention for Better Security of Human Life at Sea, or CONSEVI (*El Convenio de Concertación de Acciones para Mejorar la Seguridad de la Vida Humana en el Mar y la Actividad Pesquera en General*), which deals primarily with the safety of ship crews at sea. Although CONSEVI is not primarily motivated by security concerns, its implementation includes components that deal with improvements in communication between the ports and incoming vessels.

Mexico currently adheres to several laws related to trade and commerce. The "Law of Exterior Commerce" dictates the rules related to global trade for the nation and obligates all forms of exterior commerce to undergo the appropriate processes determined by the Secretariat of Commerce and Industrial Development *(Secretaria de Comercio y Fomento Industrial).* The law exists to promote a unified national structure for all foreign trade and reduce the amount of illegal contraband entering or exiting the nation.[569] The Mexican "Port Law" gives the federal government authority to regulate the construction, use, exploitation, and/or administration of all ports, terminals, marinas, and installations in the nation. It also gives the Mexican Armada permission to utilize port facilities under decree of the executive branch of the federal government of Mexico. [570]

Customs Regime

Organization/Hierarchy

The primary purpose of the Customs regime is to monitor and collect revenues.[571] Customs is additionally responsible for tracking and screening incoming cargo to protect against contraband and other criminal activity.[572]

Customs administration falls under the federal government's Secretariat of Finance and Public Credit *(Secretaria de Hacienda y Crédito Publico - SHCP).* The SHCP is divided into three branches. The first branch is the Secretariat of Tributary Administration (*Secretaria de Administración Tributaria - SAT*), which is the equivalent of the United States' Internal Revenue Service. The SAT's primary purpose is to collect revenues through tariffs on international trade. The second branch is the Central Administration of

Customs Operations (*Administración Central de Operación Aduanera - ACOA*), which is the central Mexican Customs office. ACOA serves as a liaison, working in coordination with the Agency of Federal Investigations (AFI) for Mexican Customs administration to facilitate secure and efficient practices at all points of entry and exit of goods. The third branch of the SHCP is the General Customs Administration (*Administracion General de Aduanas - AGA*). AGA serves as the central control of norms for Customs operations. Its purpose is to promote efficient and secure trade through the implementation of standards for all points of entry including airports, land borders, and ports.[573]

Mexican Customs operates under the Mexican "Customs Law," established in 1995 and most recently updated in 2006, which gives authority to the SHCP to regulate all Customs practices and to oversee the entrance and exit of all goods. The law outlines Customs' role as overseeing tariffs and ensuring that appropriate tariffs are charged for the particular goods being traded. The Customs Law also lists the various approved methods of inspecting goods; these are gamma-ray machines, x-ray machines, and any other technology approved by the national Customs regime.[574]

Customs Participation in Multi-Lateral Initiatives

Business Alliance for Secure Commerce (BASC)

The World BASC Organization, Inc. is an international alliance stemming from the private sector in Latin America that aims to secure the trade supply chain through facilitating cooperation between governments and international organizations. BASC has a presence in many Latin American countries, and works to establish trans-Atlantic partnerships between Customs regimes in these nations and EU member states. The organization publishes security-related information and assistance for Customs regimes and grants BASC compliance through a rigorous auditing process.[575] The BASC website states that member benefits include a reduction of trade-related risk and an improved image of private companies that meet BASC compliance standards.

Customs-Trade Partnership Against Terrorism (C-TPAT)

As discussed earlier in the report, C-TPAT[*] is a government/private partnership providing benefits to private companies that meet certain security criteria. Most importantly for Mexico, membership in C-TPAT is a pre-requisite for any business to use the Free and Secure Trade Program (FAST) instated at designated U.S.-Canada and U.S.-Mexico borders.[576]

Free and Secure Trade Program (FAST)

FAST[†] is another joint initiative between the U.S., Mexico and Canada designed to facilitate safe and secure trade between the three nations. Drivers and cargo operators

---

[*] Refer to Chapter 3 for more details on the Customs-Trade Partnership Against Terrorism.
[†] Refer to the Primer for more information on the FAST program.

that qualify for a particular level of security are able to take advantage of expedited processing and clearance at the U.S./Mexico border crossings.[577] FAST has received both praise and criticism for its driver identification program. There have been several cases of interception of contraband in vehicles operated by FAST-certified drivers. Most recently, Customs and Border Protection officials found almost one ton of marijuana in a produce truck crossing through Nogales over the U.S. border in a truck operated by a FAST-certified driver. Critics say that while FAST certification might result in expedited border clearances for companies that exhibit good behavior in commerce, it also creates loopholes through which contraband can enter with fewer inspections.[578]

Subcommittee on Customs Procedures (SCCP)

The SCCP is a sub-branch of the Asia-Pacific Economic Cooperation (APEC). The Sub-committee exists in order to "identify and pursue projects for regional enhancement of harmonized and simplified Customs procedures; projects on enforcement matters related to trade facilitation; joint projects and linkages with business/private sector organizations related to trade facilitation; and projects which will contribute to the common development of human resources."[579] Its primary goal is to facilitate strategic economic partnerships between nations of the Asian Pacific and Customs organizations in other regions of the world. Mexico, as a "partner economy" of the SCCP, commits itself to Customs modernization and increased supply-chain security measures through the organization's "12 Point Plan" for Customs regimes. Nations that commit to following through with the 12 steps must invest a significant amount of money to implement the program but, in turn, receive subsidies from the Trade and Investment Liberalization and Facilitation (TILF) Fund.[580] The TILF fund is financed by Japan in the amount of approximately $100 million over fifteen years to promote APEC-related activities.[581]

Port Case Study - Veracruz

General Port Information

The Port of Veracruz, situated on the eastern seacoast of Mexico, southeast of Mexico City, is Mexico's oldest port and accounts for approximately 20% of all Mexican imports. Veracruz is the gateway port for the majority of imports headed to Mexico City. It is also a scheduled port on a number of transatlantic services through the Gulf of Mexico with final destinations at the U.S. ports of Houston and New Orleans. Container imports account for 35% of Veracruz' total cargo breakdown, while agriculture, minerals, fluids, and vehicles make up 28%, 18%, 6%, and 4%, respectively, of total imports. The Port of Veracruz was recently named the leading Mexican port in automobile exports. In 2005, the port moved over 17,121,000 tons of cargo and led the nation in importation of agriculture, automobiles, and containers.

All port facilities are privately owned based on a concession system that allows for long-term leases of up to fifty years. The Port Authority of Veracruz (APIVER) was granted private concessions at the port in 1995 and has maintained the right to use port facilities ever since. Since its privatization in 1995, the Port of Veracruz has experienced a

significant amount of growth with incoming cargo tonnage steadily increasing over the past decade. Between December 2005 and January 2006, the port experienced a 30% increase in incoming cargo, constituting its largest 2-month percentage change in recent history.[582] Veracruz was also recently named one of the top 3 best-managed ports in Latin America by a recent UN Economic Commission for Latin America and the Caribbean (ECLAC) study.[583]

Stakeholders

Private Terminal Owners

The Port of Veracruz has five major terminals. Since implementing ISPS at the port, each terminal is now required to have its own controlled access point as well as its own security plan. Private terminal operators at the port include ICAVE, Grupo CICE, SSA Mexico, Special Cargo Terminals, Maritime Terminal for PEMEX refinery, Vopak Terminals of Mexico, Port Corporation of Veracruz, RICSA, TAMSA, and Nextel Mexico. These companies own at least a portion of one of the five terminals. In addition, there are two publicly-owned terminals that are used only for mixed goods. [584]

Veracruz' primary container terminal, comprising over 30% of all property at the port is owned by International Container Associates of Veracruz (ICAVE). ICAVE is owned and operated by the China-based Hutchison Whampoa, Ltd. Hutchison took over operation of the terminal in 1995 from the previous owners, a Philippines-based company called ICTSI and a Mexican-based organization called the ICA Group (Association of Civil Engineers). Since assuming terminal operations, ICAVE has expanded its land holdings and handling capacity by nearly one-third.[585]

For the past 11 years, ICAVE has used a private security company called the Associated Consultants of Private Security (*Consultores Asociados de Seguro Privada - CASP*). Security workers for CASP are required to undergo federal background checks. CASP employees are not armed guards, but they do carry communication devices to alert ICAVE and APIVER employees in the event of a security incident. Security at the ICAVE terminal is maintained through a continual rotation of 4 CASP employees, each of whom works 8-hour shifts, daily.[586]

A primary concern regarding ICAVE administration is the proximity of the ICAVE terminal to a very popular tourist attraction in the city. The major road that connects downtown Veracruz to this attraction runs directly behind the ICAVE terminal and is separated only by a fence. Additionally, there is a highly flammable fueling zone located on the far edge of the terminal directly beside the street. This portion of the terminal is considered one of the most vulnerable in the port by ICAVE.[587] In an interview, ICAVE employees had nothing but praise for their terminal's management by China-based Hutchison Whampoa. The employees feel that their owners are responsive and generous in providing any necessary improvements to the terminal, including security-related infrastructure needed to comply with ISPS.

In addition to terminal operators and other private companies, there are 40 global maritime lines, 250 Customs agencies, 75 companies that represent federal transport services, several railway companies, and over 30 service-provision companies that operate at the Port of Veracruz.[588]

Port Security

The port itself is situated directly adjacent to the city's downtown area and is surrounded by heavily trafficked attractions. As such, port security and controlled access points are of the utmost importance. The port currently has five points of access. The first is for personnel and allows for the passage of crewmembers and port administrators. The second allows for both vehicular and pedestrian access. The third access point, called the North Point, is located near Customs offices and inspection docks, and allows for the passage of trucks, containers, trains and federal officials. The fourth is designated only for trains. The last access point is for stevedores or other temporary workers who receive temporary identification cards at a centrally located ID center.[589]

Veracruz' current employee identification system is based on ISPS regulations. As required, each port employee is given a security-code level based on his/her role and rank at the port. Although the administration of employee IDs is handled in the central ID center, decisions are primarily made through a certification process required of all private port companies. Once a company receives its clearance, a new employee passes a minimal check process requiring him/her to provide official identification, such as a passport, and proof of employment. Workers hired by the port administration and all other employees working with sensitive security-related operations, however, undergo a more thorough process during which a background check is conducted.[590]

ISPS at the Port of Veracruz

Veracruz is fully compliant with the mandatory portion of ISPS (Part A) and adheres to certain specifications outlined in the voluntary portion of the code (Part B). The port has several upcoming security-related projects that it hopes to complete by the end of 2007. APIVER anticipates the delivery of two x-ray scanning machines to use for incoming cargo. Installation and implementation of the machines is expected to occur during June 2006 as a part of increased security measures since ISPS implementation. The Port Authority will oversee use of the new screening devices, which are expected to greatly increase the frequency of security checks at the port. However, at the time of our port visit, the Port Authority had not yet created a clearly defined implementation agenda or plan for how and when checks would be conducted.[591]

According to security officials at the Port of Veracruz, implementation of the code has brought about an increased awareness of security issues in several different ways. First, they expressed that port workers have a much clearer understanding about the importance of new security measures. Secondly, port officials credit ISPS with improved efficiency in terms of employee recognition mechanisms and access controls. Prior to ISPS implementation, identifications for employees from different terminals or with different security clearances were not clearly differentiated. Since ISPS

implementation, all terminals have their own color-coded hats and IDs that clearly state each worker's employer. A third improvement since ISPS is the creation of both port-wide and terminal-specific security plans. Last year, Veracruz conducted its first port-wide simulation of a terrorism-related security incident.[592]

Customs at the Port of Veracruz

Mexican Customs serves a dual role at the Port of Veracruz: it manages revenue and tariff collection and inspects suspicious incoming cargo. The agency's website includes a mission statement which also highlights its role in combating fraud and protecting against the importation of contraband.

Procedures

Mexican Customs recently adopted the U.S.' 24-hour rule for processing cargo manifests. This initiative helps Customs ensure that accurate information is received in a timely manner.[593] However, Customs does not yet utilize any automatic targeting technology to screen for risk factors in incoming cargo. Customs employees currently individually receive and archive manifests for all incoming cargo. Risk factors are assessed on an individual basis for each manifest and Customs employees are responsible for reporting any potentially suspicious cargo. The employee's report of a suspicious manifest follows a chain of command through senior Customs officials who have the authority to call for an inspection.

The Port of Veracruz receives the majority of all cargo manifests electronically. Customs uses Automatic System of Manifest, or SAMM-3, software that connects Customs officials to maritime agencies. The system allows Customs to see the expected date and time of arrival for each shipment as well as a description of the cargo. Ocean carriers that fail to comply with the 24-hour rule or inaccurately represent cargo information on their manifests face fines of up to $4000 per incident.[594]

One unique aspect of cargo inspections in Mexico is the requirement that representatives from several different government agencies be present at the time of inspection. In order for cargo to undergo an official Customs inspection, at least one individual from each of the following government agencies must be present: the AFI, the Mexican Armada, and the Mexican Federal Police, or PGR (*Procuraduría General de la Republica*). Of these agencies, both Customs and the AFI have the right to call for the inspection of any container, as long as they make arrangements for all necessary participants to be present at the time of the inspections. The two agencies interface with one another and share information to determine which checks should be deemed most important. In addition to these representatives, there is also a Customs official with a trained dog present at all container inspections.[595] This procedure aims to reduce corrupt dealings within the port by creating layers of security representatives that make it increasingly more difficult for contraband to enter the country.

As an example of the success of these procedures, Customs officials noted that last year they discovered over two tons of cocaine while conducting a check on an incoming

shipment. The suspicious cargo underwent a mandatory inspection based on its origin, due to a procedural mandate that requires inspections of all cargo originating from particularly problematic areas, such as Columbia. Customs credits the improved transparency of exhaustive security inspections for the successful recognition of contraband.[596]

Infrastructure

Current infrastructure for cargo inspection includes five gamma-ray machines, located at terminal exits, through which 100% of inbound cargo must pass before exiting the harbor facilities. The gamma-ray machines are overhead installations located in Customs-operated security checkpoints. These checkpoints are staffed by contracted security employees charged with checking driver identification in all vehicles that enter Customs offices or exit the port facilities en route to their next destination.[597]

Customs officials gave no clear indication as to the frequency of inspections of gamma-ray images captured at these checkpoints. However, they insisted that any suspicious scan would be set aside for an official inspection in the Customs inspection docks. Customs officials estimate that 10 to 12%, of approximately 1200 cargo manifests, are individually inspected daily through a process that compares the gamma-ray readings to manifested goods. Of these 10 to 12%, all suspicious, or heterogeneous, containers are checked.

CSI

There are currently no ports within Mexico that are considered CSI compliant. According to an official from the Mexican federal agency in charge of port oversight, Mexico has plans to implement the CSI initiative by 2008 at the ports of Veracruz, Manzanillo, Alta Miro, Progreso, Lazaro Cardneas, and Ensenada. Mexico plans to defray the cost of CSI implementation through a per-container tariff that will help provide funds for new security infrastructure.

Although Mexico's federal port oversight agency remains committed to CSI implementation, there appears to be little communication between federal decision-makers and port officials or between Mexican officials and U.S. Customs officials. According to an anonymous U.S. Customs and Border Protection official, Mexico is no longer pursuing CSI implementation at its ports and is instead focusing more attention on the C-TPAT initiative.[598] Obviously, this statement stands in direct conflict with the previous statement from Mexico's port agency.

One of the major proponents of an improved and unified security plan for Mexico is the Alliance for North American Security (*Alianza para la Seguridad de América del Norte - ASPAN*), a branch of Mexico's Secretariat of Foreign Affairs that works in cooperation with foreign governments to create a national plan for security and economic growth. The ASPAN creates reports and recommendations for all of the Port Authorities in Mexico, which include the promotion of international partnerships such as CSI.[599]

Lessons Learned and Conclusions

Over the past several years, the U.S.-Mexico trade partnership has become increasingly vital for dealing with economic, political, and security challenges in the Western Hemisphere. Mexico's role as a key player in the supply chain of U.S. imports makes the nation's security a primary concern for U.S. interests. However, there are significant differences between Mexican and U.S. priorities for global supply-chain security. While U.S. security concerns focus on the prevention of terrorist strikes, Mexico's primary security concerns relate to drug trafficking and organized crime.[600] These disparate viewpoints will create challenges to the implementation of clear and coordinated security measures that benefit both nations.

According to security officials in Veracruz, the implementation of ISPS at major Mexican ports made great strides to improve the awareness of terrorist-related security issues in Mexico. The code appears to be particularly well received by the Port Authority administrative team and by terminal operators concerned with rapid and efficient movement of cargo. Some of the notable improvements mentioned by port officials include the creation of clearly-defined security incident strategies; the creation of five specific access points; increased expenditures on security infrastructure, such as lighting and video surveillance; and improved employee recognition mechanisms, such as identification cards and terminal-specific uniforms.[601] Physical security is particularly challenging at the Port of Veracruz because of its central location and immediate proximity to major tourist hubs. Although ISPS implementation has greatly improved port security in Veracruz, some security officials expressed the need for further improvement in access controls as well as more consistency in monitoring less-trafficked areas of the port.[602]

Mexico's success with ISPS implementation stands out in direct contrast to its implementation of CSI. Currently, there are no CSI-compliant ports in Mexico, and the timeframe and credibility of implementation plans appear muddy at best. [603] There is a clear need for improved information-sharing, both internally between Mexican federal agencies and port authorities, as well as between Mexican officials and U.S. federal agents. [604]

Ensuring the fast and efficient transit of goods over the U.S.-Mexico border while securing the cargo supply chain presents an enormous challenge for both nations. The need for sustained and consistent communication between U.S. and Mexican officials remains an obstacle in creating integrated and efficient security measures that benefit both parties equally.

Chapter 10. The Netherlands and the Port of Rotterdam

Introduction

Located in Western Europe on the North Sea, the Netherlands is often considered the gateway to Europe. The Netherlands is densely populated, with a geographic area of 41,526 sq km and an estimated population of 16,407,491 inhabitants (July 2006 est.) In 2005, the country's Gross Domestic Product was US$600.8 billion*, primarily consisting of services (73.5%) and industry (24.4%). The Netherlands' largest trading partners are fellow European Union nations. Of its $365.1 billion in exports (2005), approximately two-thirds were destined for EU states: Germany (25%), Belgium (12.4%), the United Kingdom (10%), France (9.9%), and Italy (6.4%). In 2005, fellow EU states were also the leading sources of imports: Germany (17.9%), Belgium (9.9%), the United Kingdom (6.4%), and France (4.8%). The United States has a less substantial trade flow with the Netherlands. Only 4.6% of the nation's 2005 exports were destined for the U.S. At 7.6% of imports, the U.S. makes a slightly larger contribution to inbound trade. Bordering the North Sea, as well as three major European rivers, provides the Netherlands with easy access to important waterways. The country has 451 km of coastline and 5,046 km of navigable waterways. The primary ports of the Netherlands are Amsterdam, Groningen, Ijmuiden, Rotterdam, Terneuzen, Vlissingen, and Zaanstad.[605]

National Structures

Port Administration/Authority

Ministry of Transport, Public Works and Water Management

The Ministry of Transport, Public Works, and Water Management (*Ministerie van Verkeer en Waterstaat*) is responsible for transportation policy in the Netherlands. While primarily concerned with traffic and water management, the Ministry oversees the nation's ports through the National Seaports Policy 2005-2010.[606]

Netherlands Coast Guard (Nederlandse Kustwacht)

The Netherlands Coast Guard was established in 1987 through a joint agreement between the Ministry of the Interior; Ministry of Defense; Ministry of Transport, Public Works, and Water Management; Ministry of Finance and Agriculture; Ministry of Nature Management; and the Ministry of Fisheries. This agreement aimed to unify maritime responsibilities and jurisdictions in the Netherlands. In 1995, the Coast Guard was placed under the operational command of the Royal Netherlands Navy.[607] The Coast Guard is responsible for all Dutch home waters, as well as Dutch possessions in the Caribbean, Aruba and the Netherlands Antilles.[608]

* Unless otherwise noted, all currency is listed in U.S. dollars.

The two primary responsibilities of the Coast Guard are Maritime Law Enforcement and Provision of Services. Maritime Law Enforcement duties include general policing, Customs supervision, border control, upholding environmental laws and upholding nautical laws. Provision of Services includes search and rescue missions, disaster response, vessel traffic services and navigational aids.[609]

The Coast Guard is subject to annual policy plans drafted for each of its two areas of responsibility. The Ministry of Transport, Public Works, and Water Management drafts the annual policy report for Provision of Services and the North Sea Law Enforcement contact group create the policy report for Maritime Law Enforcement. The Director of the Coast Guard must create operational agreements with participating ministries in order to obtain the necessary resources and personnel to enact the policy plans. Once these agreements have been signed, the Coast Guard creates an Integrated Operational Plan that details both expectations and available resources.[610]

Koninklijke Marechaussee (KMar)

The Koninklijke Marechausee is one of four bodies of the Netherlands military. KMar is responsible to the Ministry of Defense, but primarily coordinates its work with the Ministry of Justice and the Ministry of Domestic Affairs. Essentially a police organization with military status, KMar is responsible for police duties at all of the Netherlands's airports and seaports except for Rotterdam. Duties include "turning away undesirable aliens and detaining suspects, enforcing judgments, providing emergency travel documents and the deporting of aliens to foreign authorities."[611]

Rotterdam Seaport Police

The Rotterdam-Rijnmond Police force is responsible for all policing duties at wharves, terminals or on the water within the Rhine estuary. The Seaport Police division was established in 1895 as the River Police, and has since grown to employ over 350 people. The division has a fleet of 13 vessels and 40 patrol vehicles with which it is able to monitor port activities.[612]

The key tasks of the Seaport Police are "environmental enforcement, border control, navigation-rules enforcement, port safety and security and tackling serious, organized crime." The tasks of the Seaport Police are divided into three units: Border Control, District Police, and Investigation.[613]

> **Border Control:** The Border Control Unit conducts administrative checks and risk analyses on all entering vessels before they reach the Port of Rotterdam. These procedures are conducted using the National Schengen Information System (NCIS) to process all information. The unit also checks all arriving crewmembers aboard their vessels.[614]
>
> **District Police:** The District Police Division provides general policing functions both land-side and water-side at the port. Duties include emergency response, environmental enforcement, accident assistance and vessel monitoring. District Police are divided into two units: an East unit responsible for the area between

Ridderkerk and the river Oude Maas, and a West unit responsible for the area between Oude Maas and the open sea.[615]

Investigation: The Investigation Division focuses on port-related organized crime, such as "people smuggling, drug smuggling, trafficking in weapons, and theft of, and from, containers."[616] In recognition of the international nature of many of these crimes, this Division coordinates with many other law enforcement agencies around the world.[617]

Customs Regime

Organization and Hierarchy

The Tax and Customs Administration (TCA) (*Belastingdienst*) is part of the Ministry of Finance, and falls under the authority of the Secretary of State of Finance.[618] The organization is primarily responsible for the collection of taxes; this work is subdivided among 13 regional tax offices. The TCA also maintains four Customs regions: North, West, Rotterdam, and South, each employing approximately 1,200 people. These offices are responsible for monitoring the external (non-EU) and internal (EU) borders of the Netherlands.[*] The regional offices employ a number of task-specific teams, specializing in declaration processing, customer processing and physical supervision.[619]

Statutory/Regulatory Authority

The TCA is charged with three tasks: "stopping, monitoring, and levying/collecting." The first task requires the TCA to ensure that goods such as weapons, drugs and products that might be harmful to consumers and infected animals do not enter the country. The TCA also monitors goods leaving the country, ensuring that goods are not exported to countries against which international sanctions have been levied. The second task requires the TCA to make certain that European and national Customs legislation is being properly applied, and the final task addresses the calculation and collection of owed taxes.[620]

Primary Functions

Declaration-processing teams check the accuracy of all Customs declarations and then determine the manner in which each declaration should be processed. Teams use a number of automated systems to process declarations, including the Sagitta Declaration Processing software, developed by the TCA. Customer-processing teams handle objections and appeals, issue authorizations (i.e., to process goods or to file electronic declarations), handle complaints and perform administrative audits (i.e., retrospective

[*] The 1985 Schengen Agreement and the subsequent 1995 Schengen Convention eliminated controls on internal borders between participating countries. They also established a single external frontier, at which point all incoming goods and travelers must be checked. Common rules for external border controls are defined in Article 6 of the Schengen Convention and in the Common Manual on External Borders. The mandates of the Schengen Convention were incorporated into the legal framework of the EU through the Treaty of Amsterdam.

audits of records and declarations). Physical-supervision teams inspect goods that have entered the country, check the levy of tax on those goods, and perform surveillance activities. Inspections are typically performed upon recommendation of the declaration and customer-processing teams, although physical-supervision teams may carry out inspections of their own initiative.[621] In 2004, the TCA handled nearly 11 million declarations, approximately one quarter of which, were processed electronically. Of the physical inspections performed by the TCA, 115,127 were inspections of imports and 56,932 were inspections of exports. The TCA cleared 40,000 cargoes for entry or exit by sea.[622]

The TCA's primary strategies for improving the security of Dutch ports are clustering, routing and regulation. Clustering involves the grouping of industries and companies that use hazardous materials into concentrated areas via spatial/economic policy and environmental policy. The transportation of hazardous materials is further secured through mandated shipping routes (routing) and limitation of the size of the transportation stream (regulation).[623]

Dutch Customs and the EU

The Netherlands is a member of the EU, and as such, is subject to EU border policy. Article 29 of the 1992 Treaty of Maastracht provides for cooperation between Customs agencies, law enforcement and police forces of signatory countries.[624] The EU is developing several tools to facilitate Customs cooperation. These include:[625]

- a Customs Information System (CIS) to allow national Customs agencies to better share information and assist in the prevention, investigation and prosecution of crimes;

- a Customs File Identification Database (FIDE) to prevent cross-border crimes by identifying any suspect individuals who have been the subject of investigation in another EU state; and

- Mutual institutional assistance in criminal matters, including cross-border surveillance and joint special investigation teams.

Port Case Study - Rotterdam

General Port Information

As the largest port in Europe and the third-largest port in the world, the Port of Rotterdam serves as a gateway for much of Europe. With 29,500 vessels visiting the port each year, total cargo throughput is approximately 328,000,000 tons and 7,000,000 TEUs.[626] The primary functions of the port are transshipment and transport, industry and distribution. The Port of Rotterdam has 160 different port facilities[627] which are equipped for bulk cargo, general cargo, coal ores, crude oil, liquid petroleum gas (LPG), chemicals, containers and refrigerated cargo.[628] Of the 160 different facilities, 149 terminals are fully ISPS compliant. Rotterdam's ISPS terminals are capable of handling

all types of cargo, with the exception of liquefied petroleum gas (LPG). The port expects to add an ISPS-compliant LPG terminal within the next two years.[629]

Stakeholders

Port of Rotterdam Authority

The Port Authority is the primary government entity at the Port of Rotterdam. Previously known as the Rotterdam Municipal Port Management, the Port Authority was privatized in 2004 to "create the organizational preconditions necessary for a business-driven structure with embedded political/administrative accountability."[630] The Port Authority is treated as a private corporation and, as such, adheres to the terms of the Dutch Corporate Governance Code.[631] However, shareholder ownership of the Port Authority remains with the local and national government.

The Port Authority employs over 1,300 people and is responsible for development, operations, and management at the port, as well as promotion of the port's competitive position. The two main objectives of the Port Authority are "to promote the effective, safe and efficient handling of shipping and to arrange for nautical and maritime order and safety" and "to develop, construct, manage and commercially operate the port of Rotterdam."[632]

The organizational structure of the Port Authority is divided into an Executive Board, which holds the ultimate authority, and a Non-Executive Board. The Executive Board is composed of the President (CEO), three Directorates, and one Division: the Directorate Commercial Affairs (CCO), the Directorate Finance and ICT (CFO), the Directorate Port Infrastructure and Maritime Affairs (COO), and the Division Harbour Master.[633] The Non-Executive Board is chaired by Mr. M.W. van Sluis, the Rotterdam Alderman for Economic Infrastructure, and comprises several advisory committees: Internal Audit, Participations, Human Resources, Corporate Affairs, Corporate Communication, and Corporate Development.[634]

Although the Port Authority is responsible for the daily management of the port, it leases the port's facilities to private terminal corporations.[635] The Port Authority cares for infrastructure maintenance on waterways, roads, quays and other facilities, while terminal operators are responsible for the security and efficient handling of shipping traffic.

Port Security

Due to its location at the city center, the Port of Rotterdam sees port security as an imperative. Rotterdam has instituted a port-wide security plan as well as individual security plans for each port facility. It is expected that the EU will mandate this type of planning process for all ports by mid-2007. According to the Netherlands Port Security Law, the mayor of a port city is the Designated Authority for the approval of all security plans. In Rotterdam, the mayor has delegated this responsibility to the Port Authority, Seaport Police and Customs to manage as a combined team. Because port security officials are contractors, they have not been granted Recognized Security Organization

status, which would permit them to approve terminal security plans. The Port Authority administration strongly supports prohibiting security contractors from fulfilling this duty.[636] Individual vessel security plans are approved by classification societies, such as ABS and Lloyds, which are Recognized Security Organizations.[637]

The Port Authority carefully monitors all security plans to ensure that plans are being strictly followed. In general, larger terminals have not been problematic, but occasional problems have been reported with smaller terminals. If necessary, the Port Authority may undertake random facility inspections at the behest of a port stakeholder. [638]

All security breaches and inspections are the responsibility of the Port Authority. The Port Authority developed training scenario drills for the port facilities and audits the implementation of these drills. Each port facility is required to execute a large-scale drill once every 12 to 18 months, as mandated by ISPS. In the interim between large-scale drills, occasional smaller drills help maintain high levels of security. The Port Authority itself often chooses to participate in security drills at the port's larger terminals.

Access Measures

Access is restricted within the port through a variety of measures. These measures are in accordance with the terminal-level security plans, as approved by the Port Authority, Seaport Police and Customs Rotterdam. In general, access is restricted through fencing, cameras and identification badges. The Port Administration designed biometric identification cards that are used at the Port Administration building. These badges are also available for use at the terminal level, but their usage is not required. Visitors to the port must present identification in order to receive the necessary visitors pass, which allows them to conduct business while their location is monitored.[639]

All security personnel at the port are required to have a special permit, which is issued upon completion of security training and a background check by the Seaport Police. The Port Authority requires security personnel to complete an ISPS-specific training module, in order to ensure that they fully understand the provisions outlined in ISPS.[640]

Although all port terminals are privately maintained, public quaysides do exist. Loading and unloading is not permitted at these quaysides. Should a vessel wish to dock, the requesting party must submit a special Declaration of Security to the Port Authority. The purpose of this declaration is to ensure that the docking ship follows the security plan of the quayside.[641]

Law Enforcement

Multiple government agencies coordinate to provide law enforcement at the Port of Rotterdam.[642] At the national level, the Ministry of Interior is responsible for port law enforcement. However, at the local level, the Mayor of Rotterdam is charged with port security oversight. The various law enforcement agencies that jointly participate in the port's security include the Police, Seaport Police, Fire Brigade, EPA, Medical Services, Public Prosecution, the Ministry of Transport (Inspection Department) and the Ministry of Social Affairs and Employment (Inspection Department).

Given the many organizations involved in port security, coordination is especially important. The Port Security Policy Board creates and oversees security policies during monthly high-level meetings. Additionally, all port personnel are required to undergo safety and security training. A crisis-management team, consisting of the mayor, chief of Seaport Police, public prosecution, the fire brigade, and the port authority, exists to manage any potential security situations.[643]

The Harbour Coordination Center serves as the crisis-management team's central command area. Located in the same building as the Port Authority, the center coordinates law enforcement responses to security emergencies. The center continually monitors the vessel traffic management system through large video walls. Should an unexpected situation arise, special security layers of the system will warn operators. For example, should a security level 1 ship head towards a security level 2 terminal, the center will receive live video images from a helicopter. This information will then be shared with both the police and fire departments.[644]

Additional Security Considerations

Officials at the Port of Rotterdam note that additional security improvements are always possible. Currently, Rotterdam's top priority for security improvements is the protection of water-side sections of the port. As such, improvements to water-side security measures have the full attention of key policy makers.[645]

ISPS at the Port of Rotterdam

The Port of Rotterdam implemented a security overhaul in 1994, prior to its implementation of ISPS. The 1994 restructuring of port security was deemed necessary due to recognition of the fact that organized crime units had increasingly infiltrated port activities. The security changes allowed key players in port security to work together more effectively and reprioritized security issues for port officials.

Following the 1994 changes, Rotterdam again restructured many parts of its port security in order to comply with implementation of ISPS. The Mayor of Rotterdam is the Designated Authority responsible for ISPS at the port, but he has assigned the Harbour Master as his delegate to oversee ISPS implementation. Two committees assist the Harbour Master in ISPS oversight: the Port Security Policy Board and the Port Security Committee.

According to EU port law, Rotterdam must comply not only with the mandatory Part A, but also with many of the requirements of the voluntary Part B of ISPS. Rotterdam achieved complete compliance with all ISPS requirements by the July 2004 deadline. Rotterdam defines compliance on a terminal-level rather than on a port-wide basis. The Port Authority sets the minimum standards for compliance at the port, but individual terminals are responsible for meeting all necessary requirements. The same minimum standards apply to all terminal facilities, although a terminal may choose to implement additional security measures. Because terminals are financially responsible for the costs of implementation, small- and medium-size companies have been most affected by

ISPS. In the initial phases of ISPS implementation, the Port Authority had difficulties in getting smaller companies to make the necessary investments for ISPS upgrades.[646]

ISPS requires that both terminals and ships have a prescribed level of security. At the terminal level, Port Authority inspectors conduct regular inspections of terminal facilities; inspectors conduct approximately 40 inspections per month.[647] Inspections may be carried out following notification, or at random. When severe deficiencies are found, audit teams will be sent to the facility in question.[648] Audit teams are composed of officials from Dutch Customs and the Seaport Police. All facilities must undergo a complete audit once every five years.[649] At the vessel level, any ship that is not considered ISPS compliant may be denied entry to the port or redirected to a secure location. [650]

Port Facility Security Toolkit

The Port of Rotterdam Authority, in conjunction with Aon Nederlands and KPMG Qubus, developed a Port Facility Security Toolkit to assist port authorities and terminal operators with implementation of ISPS. Two of the biggest advantages of the toolkit program are uniformity and speed. The toolkit ensures that ISPS requirements are uniformly and consistently applied across all terminal facilities. This, in turn, allows port authorities to more easily oversee and audit security implementation. In addition, the automation of risk assessments and security plans allow terminal operators to achieve compliance over a much shorter time frame. Paul Rutten, the Port Facility Security Officer at the ECT Terminal in Rotterdam, stated that without the toolkit, ECT's security plan "would have taken us months of work. We would not have been able to finish the plan before the deadline of 1 July 2004."[651]

The toolkit includes the following components:[652]

Facility Risk Assessment: Terminal operators fill out a questionnaire addressing more than 400 elements of ISPS implementation. The software is then able to create a sophisticated risk analysis of security at the terminal;

Automated Gap Analysis: Based on the results of the risk assessment, the software creates a detailed Action Plan. The Action Plan lists all remaining necessary steps to bring the terminal to full ISPS compliance;

Automated Security Plan: Following the Risk Assessment, the software produces an individualized Facility Security Plan for the terminal;

TRAM: TRAM is a Threat and Risk Analysis Matrix. This tool offers 17 different risk scenarios and provides a terminal score as well as a list of potential vulnerabilities; and

Procedure Formats: The software lists over 25 pages of detailed security procedures for each of the three ISPS-mandated port security levels.

The toolkit is adaptable to country or port-specific legislation and guidelines, facilitating its use in multiple locales. The program can also be easily expanded or adapted by the licensed users, should regulatory changes occur after implementation. The toolkit is currently used not only at the Port of Rotterdam, but also at 30 different seaports and over 600 terminals, including Belgium, France, Turkey, Lithuania, and Tanzania.[653]

Customs at the Port of Rotterdam

Customs Rotterdam is one of the four regional subdivisions of the Netherlands Customs Administration. The Rotterdam office of the TCA extends from Dordrecht, through the Port of Rotterdam, and includes the Maasvlakte. Goods both from within and outside the EU flow through Rotterdam, thus Customs officials monitor both the import and export of goods. Particular focus is given to containers and bulk goods. Any necessary audits or inspections of goods are carried out on the basis of police and Customs investigations as well as Customs legislation.[654]

Rotterdam Customs does not require advance declaration notices from incoming vessels. A general cargo manifest, crew list, passenger list, bill of lading, and other documents are all required upon arrival. Advance notice is required only for the following categories: dangerous goods of IMO class 1 and 5.2; more than 1,000 kg of other IMO classes in packages; dangerous substances in bulk including empty tankers which are not gas-free; noxious liquids; cargoes under fumigation; and fumigated cargoes with residues of fumigation vapors. For these substances, 24-hour advance notice is required.[655]

Upon a vessel's arrival at port, TCA officials use both x-ray and radiation systems to scan containers. Containers may be scanned using x-ray equipment located at Maasvlakte. Trucks, up to 19 meters long, are automatically taken via a hydraulic system through an x-ray tunnel. The entire scan lasts approximately 3 minutes. TCA officials then analyze the images from the scan, taking no longer than 15 minutes, before the trucks are cleared to continue.[656] Currently, only one terminal at the port has operational radiation screening. However, 40 additional radiation scanners are expected to come online by the end of 2006. At this point, Rotterdam anticipates being able to scan nearly 100% of all non-barge containers. The port is also in conversations with Hutchison Port Holdings regarding the possibility of installing an ICIS system, similar to one that is currently operational in Hong Kong. However, Rotterdam port officials expressed some concern over the potential quality of the images provided by this technology, due to the fact that the container does not remain stationary during the scanning process and that gamma-ray images aren't as high-density as those from x-ray scans.[657]

Megaports Initiative

Rotterdam was one of the first two ports to participate in the U.S. Department of Energy's Megaports Initiative. The cooperative agreement between the U.S. Department of Energy (DOE) and the Dutch Ministry of Finance was signed on August 13, 2003. The Megaports Initiative is a program "aimed at thwarting illicit shipments of weapons

material"[658] at strategic global ports. The DOE assists participating ports with the installation of radiation detection equipment and detection training for local Customs officers.[659]

The Rotterdam Engagement was a pilot project for the Megaports Initiative. Radiation equipment was initially installed only at the port's largest container terminal. Due to the initiative's success, Dutch officials decided to fund installations at the remaining three container terminals.[660] During the course of the engagement, the DOE trained 43 Dutch Customs officials on the new equipment. Additional training for 20 to 30 Customs officials was also provided on secondary inspection methods.[661] A recent GAO report notes that Dutch officials expressed some initial reservations about the project, due to the need to hire 40 to 60 additional Customs representatives once radiation equipment was installed at all four terminals.[662]

CSI

The Netherlands was the first European country to join the CSI program. Mr. Gerrit Zalm, Dutch Minister of Finance, signed the agreement that allows U.S. Customs agents to work at the Port of Rotterdam on June 25, 2002.[663] The first U.S. agents were deployed on August 26, 2002, and CSI became fully operational in Rotterdam on September 2, 2002.[664]

The implementation of the CSI program has caused some significant changes in Rotterdam's port operations. Although Dutch Customs did inspect outbound containers prior to CSI, the volume of outbound inspections has dramatically increased since the implementation of the program. Without the CSI program, it is unlikely that seizures of outbound cargo would have been made. Additionally, Dutch officials noted that the time-consuming nature of the implementation process was certainly the greatest cost associated with CSI.[665]

The initial implementation of CSI was not without difficulties. The Port of Rotterdam is extremely large and complex, and union regulations only allowed U.S. Customs officials to remain in Rotterdam for 3 months at a time. The frequent turnover of U.S. officials was a source of concern for Dutch Customs. Since then, these issues have largely been resolved. Presently, Dutch officials are satisfied with the existing levels of cooperation and communication.

Dutch Customs is very interested in the reciprocal nature of the CSI program. However, officials stated that goods arriving from the United States are not a pressing area of concern to them. Instead, they are more concerned with goods arriving from other parts of the world, especially West Africa. Placement of Dutch Customs officials at ports in these areas would be seen as far more beneficial than the placement of agents in the United States. Alternatively, officials would like the program to become sufficiently automated in the coming years that the physical presence of Customs agents abroad would not be necessary (i.e., cargo information could be shared electronically).[666]

Lessons Learned and Conclusions

Every port has unique strengths and weaknesses from which the U.S. can learn. Interagency cooperation is one of the strengths of Rotterdam's port administration. Port officials have strived to create open communication channels and willing collaboration among individual agencies. Port security is examined not just on a port-wide basis, but also at the terminal level. Agencies and officials have worked together to create detailed plans that meet the needs of the individual facilities.

Rotterdam's innovative approach to terminal-level security is based on its port security toolkit computer program. This program is designed to recognize threats based on specific characteristics of the facility. It also allows for regulation requirements to be systematically applied with special consideration to the unique challenges of individual terminals. The toolkit has already been marketed to the private sector and is used in other countries throughout Europe and the Middle East. However, the creation of an American version would likely require adaptations for U.S. laws and policies. The ability of this program to provide a uniform rubric for port security measures is inventive and merits further examination.

The Port of Rotterdam is not without its weaknesses, as its officials acknowledge. Weekends pose a specific challenge to security in Rotterdam. Because the port is not in operation, weekends provide an opportune time at which security could be compromised. Dutch officials are also concerned about the lack of coordination between port terminal operators. Currently, an employee fired for questionable behavior at one port facility can be rehired at another terminal. This lack of information sharing obviously weakens overall port security measures.

The Port of Rotterdam and the larger EU community share many of the U.S.' concerns over port security; however, their security priorities are often different. Rotterdam's security priorities stem from the reorganization of port agencies in 1994, prompted by the infiltration of organized crime into port activities. Since this time, security concerns have been less focused on weapons of mass destruction than on human and cargo smuggling. The Dutch believe their primary security threats come from less developed countries, particularly those in Africa.

Officials at the Port of Rotterdam are very supportive of security programs that will provide more uniform security standards throughout the world's ports. For this reason, Dutch officials have been pleased with the initial security changes brought about through ISPS. ISPS forces facilities within a port and ports throughout the world to be held to similar security standards, thereby reducing the perceived threat from ports in less secure areas. Dutch officials would like to see international measures such as ISPS carried even farther, with stricter guidelines for port security. They note that, currently, ISPS does not provide specific guidelines for the implementation of security requirements. The code also fails to explicitly define compliance, leaving ports free to define compliance by their own standards. Officials would like to see more rigorous international security legislation, with clearly defined instructions and compliance measures.

The primary recommendation of Dutch officials is the creation of terminal-level, rather than port-wide, compliance standards. A port's terminals are typically operated by different companies, and while they may seek to implement the same level of security standards, this implementation may not be consistent. By assigning appropriate security levels to individual terminals, port officials can more easily make determinations of security threats. Terminal-level compliance can then be based on individual assessments, making implementation unique to the facility in question. This standard of compliance will provide more complete security information and is believed to be the next logical step in the international effort to ensure port security.[667]

Chapter 11. South Africa and the Ports of Cape Town and Durban

Introduction

South Africa is the southernmost country on the continent of Africa. Its total geographic area is 1,219,912 sq km, slightly less than twice the size of Texas. At present, South Africa has a population of 44,344,136. However, with a current HIV/AIDS rate of 21.5%, future demographics are highly uncertain. South Africa's economy is one of the most robust on the African continent. In 2005, it had a Gross Domestic Product of US$527.4 billion*, the 24th largest GDP in the world. Exports and imports amounted to $50.91 billion and $52.97 billion, respectively. With 10.2% of total exports, the United States is the leading consumer of South African goods. The U.S. is also the second-largest source of imports, providing 8.5% of imports in 2005. South Africa has 20,872 km of railways and 275,971 km of roadways.[668] There are seven working commercial ports in South Africa; an eighth port is currently under construction.[669]

Durban – Durban is South Africa's busiest container port. The port moved 1.4 million TEUs in 2002.

Cape Town – Cape Town is a multipurpose port, and a large importer/exporter of fruit. The port also has a sizable container facility that processes 610,000 TEUs per year.

Richard's Bay – The Port of Richard's Bay boasts the largest bulk coal terminal in the world.

Saldanha – Saldanha is mainly notable for its crude oil importing capabilities.

Port Elizabeth – Port Elizabeth is a general, multi-purpose port.

East London – The Port of East London is the only commercial river port in South Africa.

Mossel Bay – Mossel Bay is a small specialist port.

Nggura - The Port of Nggura is currently under development.

* Unless otherwise noted, all currency is listed in U.S. dollars.

National Structures

Port Administration

A number of government agencies are involved in South Africa's national security. The following descriptions pertain mainly to their respective areas of jurisdiction over port security.*

National Department of Transportation (DoT) – DoT is the government agency with jurisdiction over transportation infrastructure. Port security oversight is a part of this responsibility.

Transnet – Transnet is a private company, however, the South African government is its major shareholder. The company comprises nine divisions - Spoornet, the National Ports Authority (NPA), South African Port Operations (SAPO), Petronet, FreightDynamics, Propnet, Metrorail, Transtel and Transwerk. Transnet also has several subsidiary companies, most notably South African Airways (SAA).[670]

National Port Authority (NPA) – NPA is the landlord agency for South African ports. It is responsible for port management, port control and port security operations.[671]

South African Port Operations (SAPO) - SAPO manages 13 cargo terminals, located at six different South African ports.[672]

South African Maritime Safety Authority (SAMSA) – SAMSA serves the maritime industry by ensuring safety of life at sea, preventing pollution and providing some port services. SAMSA has the right to board ships in order to check compliance with maritime safety and pollution standards.[673]

South African Police Service (SAPS) – SAPS is responsible for law enforcement and use of force (detention, arrest powers). South African police have jurisdiction over law enforcement at border points of entry and ports.[674]

National Intelligence Agency (NIA) –The NIA was responsible for creating South Africa's standards and procedures for ISPS compliance. The agency continues to provide intelligence information and consultation services to aid ports with compliance measures. [675]

South African Defense Force: Navy (SANDF) – SANDF enforces South Africa's maritime laws and borders. The Navy serves primarily as a coastal defense force; it performs Maritime Interdiction Operations and enforces fishing

* As of April 19th, South Africa is currently overhauling their port security operations and organizational structure. For the purpose of this project, the NPA will still be treated as the primary port security administrative body.

laws. Although SANDF is not significantly involved in port security, it may be called in as a last resort for port security operations.

South African Revenue Service (SARS) – SARS is the Customs agency of South Africa.

Though all of the agencies listed above are involved in port security, the two agencies most involved in container security are the NPA and SARS. These agencies will, therefore, be introduced in greater detail.

Port Authority

The NPA is a division of Transnet, the enterprise responsible for much of South Africa's transportation infrastructure. The NPA is the landlord of the South African ports and most of South Africa's port security responsibilities fall to this agency.* The stated mission of the NPA is "to create and sustain world class freight and logistics solutions."[676] The company divides its activities into two businesses, Landlord services and Maritime services. The Landlord business involves infrastructure management and maintenance, optimizing port usage and safety of the port environment.[677] The Maritime business includes dredging, lighthouse services, ship repairs and general maritime services.[678]

The NPA is also in charge of ISPS implementation in South Africa. South Africa became fully ISPS compliant on June 28, 2004, before the international deadline of July 1, 2004.[679] Nozipho Sithole, General Manager of Operations, describes the NPA's approach to ISPS implementation as being "all about holistic and cohesive risk management, identifying threats, and vulnerabilities, involving the port communities and filling the identified gaps."[680] Port security falls under Mrs. Sithole's Operations Management Division. Within this division, Kerwin Rampono is the Head of National Maritime Security Operations.[681]. Per ISPS, each port must have a Port Security Officer (PSO); these officers report directly to Mr. Rampono. Each PSO must ensure his/her port is compliant with ISPS[682] through individual port security plans. Although the PSO is the NPA authority in charge of security for each port, the law enforcement role still falls to the police. The NPA and SAPS try to closely coordinate on all port security issues.

Customs Regime - SARS

As outlined in the South African Service Act of 1997, the objective of South Africa's Customs regime is "the efficient and effective collection of revenue."[683] The Service Act created an "an organ of state within the public administration, but as an institution outside the public service."[684] The agency's main functions are to collect all revenues that are due; ensure maximum compliance with the legislation; and provide a Customs service that will maximize revenue collection, protect the borders and facilitate trade.[685]

---

* There is current legislation being drafted that would relieve the NPA of much of its responsibility for port security. Instead, a separate security hierarchy or organization would be established.

Though SARS has the power to levy fines, a police presence is required to carry out law enforcement duties and arrests.

SARS contributes to container security through its responsibilities with the CSI program. The Port of Durban is the only CSI port on the continent of Africa. South Africa's participation in the CSI program is driven by two main considerations. First, the country desires to strengthen relations with its largest trading partner. The SARS website states: "SARS understands the impact which CSI has on the export business sector and is moreover conscious of the need to expedite the means to facilitate this leg of trade to ensure continuity of trade with the U.S. and other major destinations in the world."[686] Secondly, South Africa believes CSI will help improve its national security and facilitate legitimate industry. SARS hopes to "extend the effort and benefits which can be attained through future CSI participation to the local environment. In this regard security and control mechanisms at our troublesome land borders and transit areas can be addressed simultaneously."[687]

Currently, SARS is leading an aggressive campaign to combat smuggling, human trafficking, drug re-distribution, counterfeiting and money laundering. This campaign's goal is, in part, to recover lost revenue, but also to allow legitimate commerce to flourish and to increase overall security. As a part of these efforts, South Africa has recently purchased several new container scanners. Four of these new container scanners were placed at the Port of Durban; the remaining scanners were spread out among other locations.[688]

Port Case Studies – Cape Town and Durban

This case study is based on a port visit made to Cape Town on January 9, 2006. However, supplemental information taken from the port visit to Durban on January 10, 2006 is included and annotated as such in the text.

General Port Information

The Port of Cape Town consists of four main areas:[689]

Victoria Basin – This area contains the Victoria and Alfred Waterfront. The waterfront is a large tourist attraction consisting of shopping malls, restaurants and bars. All cruise ships smaller than 200 meters dock in this area, and the waterfront also offers space for small commercial vessels and fishing trawlers;[690]

Alfred Basin – Located to the Southwest of Victoria Basin, both the Robinson graving dock and synchrolift are located at this site;[691]

Duncan Dock – This location facilitates most of the break bulk and bulk cargo. Shipping berths A through M are located at this site. The A berth is used for oil, rig repairs and other oil-related activities. Berths B through E are predominantly used for the export of fresh fruit. Berths E and F also accommodate large cruise ships. The repair quay, dry dock, and crude oil terminal are also located in

Duncan Dock. Of special note is the Yacht basin, the location of the Royal Cape Yacht Club;[692] and

Ben Schoeman Dock – Cape Town's container terminals are located at this dock. The 500-level berths are used for offshore activities, 600-level berths are used for container traffic and the 700-level berths are used for lay-up traffic. Railway access is available in the container offload areas.[693]

Cape Town has a wide spectrum of port stakeholders. SAPO operates all of the port's container terminals, as well as some of the unloading berths at the Duncan Dock. The Victoria and Alfred Waterfront is partially owned by private enterprise, and the NPA assumes landlord functions throughout the remainder of the port. There are also numerous private facilities and services offered throughout the port, ranging from fresh produce services to engineering services.[694]

Cape Town's official container terminal capacity is 600,000 TEUs per year. However, the port is currently running overcapacity at 610,000 TEUs per year. An expansion plan is being formulated that would upgrade its container capacity to 1.6 million TEUs.[695]

Port Security

Prior to 9/11, South Africa's primary security priorities were petty crimes, human and drug trafficking, and Customs control. More recently, South Africa has begun to take a broader and more inclusive view of security. Nozipho Sithole details this change:

> "We had become experts at managing financial risk, legal risk, or risks that come with dissatisfied customers. Safety, however, had lagged behind. The focus was on theft avoidance or preventing stowaways from having access to sea-going vessels. We now appreciate that safety and security have a direct impact in minimizing or preventing customer loss, employee flight, or the financial death of an organization."[696]

The implementation of ISPS has forced South Africa to change its approach to security in a relatively short span of time; many security practices are still being reorganized.

Physical Security/Restricting Access

The Port of Cape Town (CPT) has limited technology and equipment at its disposal. Currently, the container terminal has full camera coverage and most of the Duncan Dock is also under surveillance. At this time, closed circuit television (CCTV) is not being used for camera coverage. However, the port hopes to install a CCTV system, with a CCTV control room, within the next year and a half. Once this new system is installed, the harbor master, the port security officer and other specified port managers will all be able to access the cameras.[697] A CCTV control room is already being built at the larger port of Durban.[698] All of South Africa's ports are also investigating additional security technologies, such as pop up barriers, intruder detection devices, and information technology upgrades.[699]

At the Port of Cape Town, primary access control occurs at the individual facility level. The container terminal employs an additional fence and checkpoint where trucks and visitors are thoroughly scrutinized. Entrance to the actual container facilities requires documentation, such as manifests, ID, shipment dates/assignments, etc. Various port facilities fall outside ISPS designations; however, Cape Town has integrated these facilities into the overall port security plan. Cape Town also employs secondary access controls through perimeter fencing. The entire perimeter of the port is fenced, allowing for better traffic control. Cape Town has three perimeter access points at which guards require vehicles to stop and show identification. These checks are secondary access measures, and as such, are not as high-level as those conducted at the individual facilities.

Personnel and Training Requirements

Security personnel in Cape Town consist of private security companies and "in-house" security provided by the NPA. Neither the "in-house" personnel nor the privately hired personnel have the power to detain or arrest. If a security incident occurs, SAPS is contacted to exercise the actual enforcement of the law. Police are present both land-side and water-side at the port, but waterborne capabilities are very limited at this time.

Cape Town has a very low turnover of security personnel. Competent security officers often stay on for many years.[700] This fact cannot be attributed to job prestige; instead, it is more often due to financial necessity. With unemployment hovering at 25% in South Africa, jobs are at a premium.[701] Private contractors, however, are not compensated equally with government security personnel. The superior wages and increased oversight of NPA officers typically results in greater reliability and effectiveness. Private contractors are paid far less than government security, oftentimes below the minimum wage. As a result, private security has typically been less reliable; some employers have reported exceedingly high absentee rates.[702] South African security personnel realize that the current organizational formation is inefficient and redundant and they hope to implement changes in the future. The best solution to this problem would be to enlarge the government security force and decrease contract security.[703] This change will be dependent upon funding and the upcoming reorganization of port security responsibilities. Also, as South Africa updates its security technology, there will be a decreased demand for manpower.

Training of security personnel in South Africa is done largely "on-the-job." The South African Qualifications Authority mandates standards through a system that assigns personnel to a rank ranging from 1 to 8. Levels 6 through 8 are equivalent to college, masters and Ph.D.-level expertise in security, respectively. There is some frustration with this system, due to the limited time it takes to reach the manager level 5 (as little as 6 months). Experienced personnel often find themselves ranked at similar levels to far less experienced workers.[704]

As a part of its paradigm shift from pre-ISPS to post-ISPS standards, South Africa is developing a program to better empower and provide customer service training for security personnel. When port visitors/clients enter the port, security officers are

invariably the first point of contact, thus South Africa believes this training is important to promote both business and security. Security and customer service centers are currently being developed.

Security Plans

Per ISPS requirements, the Port Security Officer (PSO) is in charge of Cape Town's port security plan. ISPS also mandates that each port facility appoint a port facility security officer (PFSO); these officers report to the PSO. The PSO oversees compliance to the port security plan through periodic visits to individual facilities and their PFSOs. The Yacht Club and the Victoria and Alfred Waterfront pose some logistical difficulties for Cape Town's security plan. The Waterfront is included in the port security plan, and the area maintains its own security staff that report to the PSO. However, there are no security checkpoints or fences surrounding the Waterfront area, allowing visitors direct entrance to the area's shops and restaurants. In contrast, the Yacht Club is located deep in the Duncan dock, behind the secondary port security fences. This location causes a constant struggle between the need for security and accessibility for the club's guests. At present, guests must be on an approved list to gain entrance and are checked at the perimeter port entry points.

Coordination with Various Law Enforcement Agencies

Coordination among the various agencies involved in port security has improved as South Africa's security policies have evolved. Various national-level entities, such as the National Intelligence Coordinating Committee[705] and the Private Security Regulatory Authority[706], have facilitated this coordination. Sub-Saharan regional coordination and communication has been initiated through the Southern African Development Community (SADC), but plans for this coordination remain in the beginning stages.[707]

Although inter-agency communication has improved, South Africa still faces many challenges in this area. Ship captains have expressed some frustration and confusion over port entrance procedures.[708] Currently, ships must interface with SAMSA, the NPA (Harbor masters), Customs, and SAPS. Entering vessels must contact SAMSA, who then sends the vessel information to the Maritime Security Coordination Center. At this point, the vessel's information is scrutinized by multiple agencies, ranging from the NIA to Foreign Affairs.[709] Once in port, the NPA has jurisdiction over vessel security. However, should an incident occur or should a search be required, action must be taken through the on-site SAPS. Both Cape Town and Durban recognize the need for a command/coordination operations center and are working towards this goal. Durban has already established a Port Security Operations Committee that is responsible for coordination between the NIA, SAPS, SARS, SAMSA and the NPA. Additionally, a common database is being developed to ease the redundancy associated with the current paper-driven process.[710]

Future Security Improvements

South Africa is committed to working towards further security improvements at its ports. The following are some of the predominant goals mentioned by government officials:

- Empower non-SAPS personnel with search, seizure, and arrest powers;
- Develop a Portal information system similar to the U.S.' Automated Commercial Environment database/coordination system;
- Establish operational/tactical command centers at the ports;
- Increase security technologies;
- Institute a security-oriented mindset infused with business at all levels;
- Create new security organization regulations to increase efficiency (to include closer partnerships among agencies); and
- Empower security personnel by including them in a dual port/business role.

ISPS at the Ports of Cape Town and Durban

Pre-Implementation Practices

Prior to ISPS implementation, South Africa's security practices were not as clearly established or comprehensive as they are today. South Africa did not have a national level guidance for port security; instead, security was handled at the individual port level. Inter-agency operational cooperation was not well established, and port-wide security features such as perimeter fencing were not used. In spite of this, South African security was generally well regarded prior to ISPS, and has only improved upon its reputation since implementation.[711]

Post-Implementation Practices

The largest obstacle to South Africa's implementation of ISPS was the lack of specificity or guidance provided by the code's mandates. In South Africa, the NIA was charged with the responsibility of drafting the national ISPS code procedures. [712] The major complaint and difficulty agency officials expressed was that the wording of the international ISPS code guidance was extremely vague. Additionally, officials struggled with the lack of a prior model or successful implementation after which they could model their own procedures.

Following South Africa's completion of its compliance code, ISPS implementation required major investments of infrastructure, manpower and capital. Additionally, large-scale training initiatives were required in order to familiarize employees with the new ISPS requirements. Officials were again frustrated and disappointed that training was

not offered by international institutions. South Africa lacked personnel with the necessary expertise and experience to lead an immense security overhaul. Planners were largely creating security procedures and organizations from the ground up. As a result, port officials believe they expended scarce time and resources unnecessarily because international guidance and best practices were not provided. Lack of international guidance not only caused some difficulties with implementation, but also led to resentment at the rate with which these vast security changes were being brought about. However, following implementation, South Africa's national security leadership has been able to increase the efficiency of national security plans and the cohesion and communication between security agencies.

Currently, South Africa is fully compliant not only with the mandatory ISPS Part A guidelines, but also with those in the voluntary Part B. South Africa's national regulations also expand upon ISPS requirements to include vessels weighing less than 500 tons. All ships between 25 and 500 tons belong to a single classification, and any remaining ships below 25 tons are included in their own classification group.

Recommendations for the Future

During the Cape Town and Durban interviews, South African officials offered many suggestions for improvements to ISPS. The following points are items of note and accompanying recommendations.

- ISPS needs a legal framework to provide for better code enforcement measures.[713] This issue is especially important when compliance problems occur with international organizations. South African officials reported that many non-compliant ships enter their ports. Due to the nature of South Africa's current security and economic status, most ships are still allowed in, but are reported to the proper international authorities.[714] South Africa's frustration over this issue was especially profound when a U.S. vessel that was not ISPS compliant entered South African waters without proper documentation of hazardous materials.[715]

- The need for better information sharing was expressed during each stakeholder interview. South African officials would like to see the creation of an international database information system. Such a database would allow national security officials to cross-check information, and increase the efficiency of national security agencies.

- An international body, such as the IMO, should facilitate security training both at the strategic and operational levels. An international organization would be able to provide training personnel to all requesting countries around the globe. This training would expedite the training process for countries such as South Africa. Without such leadership, South Africans feel as though they are being forced to invent processes that could be more expeditiously learned through training. Australia and the United Kingdom have already worked with South Africa to provide such training; the U.S. is in the process of arranging reciprocal ports visits to exchange best practices.

- Ships below 500 tons should be included in ISPS regulations. These vessels frequently travel internationally, but yet are not required to adhere to ISPS. South African officials view these ships as a greater threat than large vessels, because smaller vessels are often more easily accessible for terrorists.[716]

- Underwater threats, while expensive to deter, need to be addressed.[717]

- South Africa would like to increase the scope of ISPS code to include facilities outside of the ports. For example, Cape Town is considering the inclusion of the port industrial park in its ISPS security plan.[718]

- Integrate programs such as CSI and C-TPAT into ISPS. Required training for these programs could be included as an annex to ISPS. South African leaders believe consolidation of the various programs would lead to greater efficiency and understanding. South Africa is currently planning to develop its own supply-chain security system similar to C-TPAT.

- South Africa struggles with securing the necessary funding for security upgrades. They would like to see an international body provide a fund for security improvements in developing countries. Leaders noted that if the international community would provide more help to less developed countries, there would be a greater effort to comply and excel at security affairs.

- The focus of ISPS is a source of concern to South Africa. Because the code was largely created by the U.S., its focus is on terrorism. Many other countries worry far more about crime than terrorism. South African leaders feel that although ISPS does help crime prevention, it may be alienating Muslims who perceive its focus to be on combating Islamic fundamentalist terrorism.[719]

Customs at the Ports of Cape Town and Durban

Vessel/Cargo Clearance

Processing statistics, seizure, and enforcement data could not be acquired by the time this report was written. However, Customs reporting procedures can be accessed from the SARS website and through the Lloyd's Register-Fairplay Ltd. The complete procedural guide is extensive and outside the scope of this report.

Currently, SARS is transitioning from a paper-based to a computer-based system, known as the Manifest Acquittal System.[720] The Electronic Database Interface is a computer program through which manifest data can be shared. Ship and manifest information can also be shared over the SARS website.

Agency Interface and Security Roles

Though Customs is an autonomous organization of the State, it does not have search and seizure powers; its powers are relegated to fines and judicial enforcement. If a search or seizure is warranted, SAPS is required.

At present, Durban is the only South African port with an X-ray scanner. However, approximately 60 to 80 new scanners are being procured at this time.[721] Once the scanners are acquired, they will be strategically placed throughout the country. SARS will have responsibility for oversight of the new scanners.

CSI

Currently, Durban is the only CSI-compliant port in Africa; Durban achieved compliance on December 2, 2003.[722] U.S. Customs has agents in Durban that work closely with SARS through a business intelligence liaison. SARS officials consider the program to be a success and do not feel port efficiency has been hindered.[723]

South Africa is interested in the reciprocity of CSI, but officials do not anticipate that security threats will come from vessels of U.S. origin. A prominent idea mentioned during port interviews was to incorporate CSI into ISPS. This would allow SARS agents to initiate reciprocal programs at ports that have greater security significance than U.S. ports, specifically ports in East Asia.[724] Officials also expressed interest in the development of an international Customs model based on the CSI program.

Lessons Learned and Conclusions

South Africa is important to global port security because of its geographic position, experience with ISPS compliance, inclusion in CSI, and because it is considered a prominent leader on the continent of Africa. South Africa's strategic location makes it a viable trade portal for much of sub-Saharan Africa and a vital waypoint for international commerce. The country provides an outstanding example of how CSI can successfully operate abroad and, due to its economic prosperity and democratic principles could provide the valuable security leadership the African continent needs.

South African authorities believe that ISPS is a valuable tool for improving port security. However, they feel the code was burdensome to implement, due to the lack of training or guidance and the expedited time requirements.[725] The lack of specificity in the code's guidance was especially frustrating. Although South Africa was able to comply with the code, compliance placed a definite strain on the country's resources. In order to avoid similar situations, developed countries need to increase their understanding of the unique struggles faced by developing countries. It is especially difficult for developing countries to marshal the economic resources and manpower required to achieve international compliance. Scant resources, whether professional, economic, or political, can make the necessary security transitions especially difficult. Developed nations must work to prevent creating a negative view of "forced" security in nations that have difficulty implementing such procedures. Additionally, international institutions or nations such as the U.S. should provide training and leadership to assist less developed nations with compliance. South Africa's experiences with ISPS implementation highlight the necessity of these measures. South Africa is far more developed and economically stable than many other African nations, and yet, it still found the changes mandated by the international security system difficult to implement.

South Africa believes greater international cooperation will improve efficiency and effectiveness not only in its own security affairs, but also on a regional and international scale. South Africa is seen as a leader in sub-Saharan Africa and plays an important role in many regional issues, including port security. Despite the country's difficulties with the security transition, South Africa has been relatively successful in its implementation of ISPS. Leaders recognize the importance of secure ports and supply-chains to the economic vitality of their nation. This mindset, and the country's implementation of international standards, makes South Africa a valuable strategic asset with the potential to proliferate security throughout the SADC and the continent of Africa. Any proliferation of security standards in Africa will not happen without increased funding, training, information sharing, technology sharing, and increased diplomatic cooperation from the international community. As countries such as South Africa increasingly integrate security measures into business and government operations, the U.S. and the rest of the industrial nations need to foster this paradigm shift with thought and consideration.

List of Acronyms

ABRATEC *(Brazilian Association of Public Use Container Terminals)* (Associação Brasileira dos Terminais de Conteineres de Uso Público)

ACE *(Automated Commercial Environment)*

AEO (*Authorised Economic Operator*)**:** a supply-chain secured shipper, carrier or intermediary private sector participant in the WCO Framework.

AES *(Automated Export System)*: a system that allows shippers or their agents to provide shipment data electronically to Customs. Its automatic editing feature helps to ensure compliance with export regulations and data requirements of various federal agencies.

ALADI: (*Latin America Integration Association)* (Associação Latino-Americana de Integração).

AMS *(Area Maritime Security)*: for more details, see section three of chapter three.

APEC *(Asia-Pacific Economic Cooperation)*: a forum that helps to promote and regulate liberal trade and economic policies throughout the Pacific Rim.

ATS *(Automated Targeting System)*: a U.S. Customs and Border Protection system used to evaluate the risk level of shipments to help identify which ones should be inspected. It applies a set of weighted rules to information provided in bills of lading to assign risk scores to incoming shipments.

BASC *(Business Anti-Smuggling Coalition)*

BPC *(Bharat Petroleum Corporation Limited)*: operates the liquid cargo terminal on a B-O-T basis with Jawaharlal Nehru Port Trust in India.

C&ED *(Customs and Excise Department)*: oversees the flow of all goods in and out of Hong Kong.

CAMEX (*Foreign Trade Council)* (Camara de Comércio Exterior): an official organ of Brazil, presided over by the Ministry of Development, Industry and Foreign Trade that accompanies and monitors foreign trade and security activities such as C-TPAT, CSI, ISPS and the U.S. Bioterrorism Act in addition to measures emanating from ALADI and Mercosul.

CBEC *(The Central Board of Excise and Customs)*: a Board within India's Department of Revenue that formulates policy concerning levy and collection of customs and central excise duties, prevention of smuggling, and administration of matters relating to Customs, Central Excise and Narcotics.

CBP *(U.S. Customs and Border Protection)*

CCTV *(Closed Circuit Television)*

CES (*French Customs & Excise Service)*: the National Customs agency of France, reports to the Minister of Finance, Economy and Industry.

CESPORTOS *(State Commissions for Public Security at Ports, Port Terminals and Navigable Waterways)* (Commissões Estaduais de Segurança Pública em Portos, Terminais e Vias Navegáveis): responsible for evaluating Brazil's port risk assessments and security plans and submitting to CONPORTOS for approval.

CIP (*Carrier Initiative Program)*.

CISF (*The Central Industrial Security Force)*: a force established under India's Central Industrial Security Force Act of 1968 (50 of 1968), comprising 2,800 troops to protect the nation's economic wealth, mainly with Public Sector Undertakings.[726] It is now one of the nation's most prominent defense forces.

CITES (*Convention on the International Trade in Endangered Species of Wild Flora and Fauna)*: an international agreement drafted as a result of a 1963 resolution adopted at a meeting of members of the World Conservation Union (IUCN). Its aim is to ensure that international trade in specimens of wild animals and plants does not threaten their survival and accords varying degrees of protection to more than 30,000 species of animals and plants.

COANA *(Coordinator General of the Brazilian Customs Service)* (Coordenador Geral de Administração Aduaneira): Responsible for administering Brazilian Customs' security measures

CODESP *(Port Authority for the State of São Paulo)* (Companhia das Docas do Estado de São Paulo): CODESP is also known as the Santos Port Authority. Santos is South America's largest port.

CONPORTOS *(National Commission for Public Security at Ports, Port Terminals and Navigable Waterways)* (Comissão Nacional de Segurança Pública em Portos, Terminais e Vias Navegáveis). Brazil's inter-ministerial body responsible for implementation of the ISPS Code, comprising membership from the Ministries of Justice, Finance, Transportation, Defense, and Foreign Relations.

COTP *(Captain of the Port)*: as required by MTSA.

CSI (*Container Security Initiative)*: An initiative launched in 2002 by the U.S. Department of Homeland Security's Bureau of Customs and Border Protection, to increase security for cargo shipments bound for the United States.

C-TPAT (*Customs-Trade Partnership Against Terrorism)*

DHS *(U.S. Department of Homeland Security)*

DoS *(Declaration of Security)*: for more details, see section three of chapter three.

DPI *(Dubai Ports International):* one of Hong Kong's container terminal operators.

E.U. (*European Union):* an intergovernmental, supranational union of 25 democratic member states from the European continent.

FAST *(Free and Secure Trade)*

FMSC *(Federal Maritime Security Coordinators)*: as required by MTSA; for more details, see section three of chapter three.

FSO (*Facility Security Officer)*: as required by MTSA; for more details, see section three of chapter three

FSP *(Facility Security Plan)*: as required by MTSA; for more details, see section three of chapter three.

GATT (*General Agreement of Tariffs and Trade*): a Customs valuation agreement which determines the value of goods for Customs duties and taxes.

GTP-Portos (*Permanent Working Group for Ports)* (Grupo de Trabalho Permanente): an arm of the Ministry of Transportation tasked with accompanying and monitoring the emergency activities and priority actions of Brazilian port policy.

HIT *(Hutchison International Terminal)*: one of Hong Kong's container terminal operators.

HKCTOA *(Hong Kong Container Terminal Operators Association)*: a private association formed by the private container terminal operators in Hong Kong. The goal of the HKCTOA is to promote Hong Kong as a container shipping port.

HLSG *(High Level Strategic Group)*: a 12-member country strategic planning group formed by the WCO to create and implement the Framework.

HPH *(Hutchison Port Holdings)*: the world's largest independent terminal operator and a subsidiary of Hutchison Whampoa, LTD.

ICIS *(Integrated Container Inspection System)*: a multi-tiered system of container inspection developed by SAIC, which allows terminal operators to inspect all containers entering and leaving their facilities.

IMO *(International Maritime Organization)*: an international organization concerned with the maritime industry.

IPP *(Industry Partnership Programs)*

ISO *(International Organization for Standardization)*: an international standard-setting body that produces and promotes world-wide industrial and commercial standards. The

non-governmental organization consists of other international organizations, countries and private sector participants. In November, 2005, the ISO published the first in a series of supply-chain security recommendations, ISO 28000 and 28001.

ISPS (*International Ship and Port Facility Security Code)*: a two-part legislative amendment to the 1974 Safety of Lives at Sea Convention, describing minimum requirements for ship security.

JNPCT *(Jawaharlal Nehru Port Container Terminal)*: the container terminal operated at the JNPT.

JNPT *(Jawaharlal Nehru Port Trust):* the 11th Major Port Trust in India commissioned by the Central Government on 26 May, 1989.

LTL *(Less-than Truckload)*

MARSEC *(Maritime Security):* an abbreviation for three maritime security levels; for more details, see section three of chapter three

MDIC *(Ministry of Development, Industry and Foreign Trade)*(Ministério de Desenvolvimento, Indústria e Comércio Exterior)

MIC *(Hong Kong Maritime Industry Council)*: an advisory council to the Economic Development & Labour Bureau whose purpose is to advise the Bureau on the "formulation of measures and initiatives to further develop Hong Kong's maritime industry."

MPT (*Major Port Trusts)*: the administrative authority for major ports in India. The authority is embedded in a Board of Trustees. The Central (Federal) Government transferred all assets and liabilities to Boards of major ports.

MPTA *(Major Port Trusts Act, 1963)*: an act to make provision for the constitution of port authorities for certain major ports in India and to vest the central administration, control and management of such ports in such authorities.

MTSA (*Maritime Transportation Security Act)*: U.S. minimum security standards initiated after 9/11.

NDoT (*National Department of Transportation)*: administers South Africa's transportation infrastructure. It is also ultimately responsible for port security.

NIA *(National Intelligence Agency)*: provides intelligence information and consultation services to the ports for code compliance and wrote the ISPS code for South Africa.

NITL (*National Industrial Transportation League)*

NPA *(The National Port Authority)***:** in charge of port management, port control, and acts as the landlord agency for South African ports. Port security operations currently fall under its jurisdiction.

NSG *(National Security Guard)*: a Federal contingency deployment force to tackle all facets of terrorism in the country.

NSICT *(Nhava Sheva International Container Terminal)*: India's first privately managed container terminal. It is run by P&O Ports a subsidiary of the Peninsular and Oriental Steam Navigation Company, UK, which was recently bought by Dubai Ports World.

NVOCC (*Non-Vessel Operating Common Carriers)*

OGMO (*Brazil's Casual Stevedores and Permanent Dockworkers Management Body)* (Órgão Gestor de Mão-de-Obra)

PASAC (*Port Area Security Advisory Committee*): a consultative committee tasked with advising the Marine Department "on all matters relating to the implementation of the IMO's ISPS in the Hong Kong Special Administrative Region including port area security requirements, ship/port interface matters and to monitor the application of ISPS Code after 1st July 2004."

PDC *(Hong Kong Port Development Council)*: an advisory committee that provides advice to the Chief Executive on all aspects of port planning and development.

PFSWG *(Port Facility Security Working Group***)**:an interdepartmental working group, which serves as the executive arm of the Marine Department in enacting the port security requirements of ISPS. In addition, the PSFWG has "the responsibility of assisting port facility operators to carry out their own security assessments and prepare security plans" for approval by the Marine Department.

PAM *(Port of Marseille Authority)*: France's largest port, situated on the French Mediterranean seacoast.

PROHAGE (*Brazil's National Commission for Harmonization of Activities of Agents of Authorities in Ports)* (Comissão Nacional de Harmonização das Atividades dos Agentes de Autoridades nos Portos): a Commission that works to integrate port activities and optimize dispatch of ships, cargo, crew and passengers.

PSCG *(Private Sector Consultative Group)*: a 30-member private sector advisory group formed to guide implementation of the WCO Framework.

RSO *(Recognized Security Organization)*

SAFE *(WCO's SAFE Framework of Standards to Secure and Facilitate Global Trade)*: an international Customs and private sector initiative to modernize Customs administrations and secure the global supply chain to facilitate trade.

SAIC *(Science Applications International Corporation)*: the largest employee-owned engineering and research company in the USA.

SAMSA *(South African Maritime Safety Authority)*: serves the maritime industry by ensuring safety of life at sea, preventing pollution, and some port services. SAMSA can board ships to check compliance with maritime safety and pollution standards.

SANDF *(South African Defense Force: Navy)*: enforces the laws of the sea. Not especially involved with port security, it is mainly a coastal defense force. It performs Maritime Interdiction Operations and enforces fishing laws. SANDF may be called in as a last resort for port security operations.

SAPO *(South African Port Operations)*: manages 13 cargo terminal operations situated across six South African ports.

SAPS (*South African Police Service)*: through various divisions, SAPS is responsible for actual enforcement of laws and use of force (detention, arrest powers). This includes the borders and ports (points of entry).

SAR *(Special Administrative Region)*: this designation makes Hong Kong an administrative division of the People's Republic of China, with a great deal of special autonomy. As an SAR, Hong Kong retains its own separate political and economic system, and complete control over all issues of state except national defense & diplomatic relations.

SARS *(South African Revenue Service)*: South Africa's Customs agency.

SCS (*Supply-chain specialist*)

SENASP *(National Secretariat for Public Security)* (Secretaria Nacional de Segurança Pública): a branch of Brazil's Ministry of Justice tasked with directing CONPORTOS.

SINDIMAR *(Maritime Navigation Agencies' Syndicate of the State of São Paulo*) (Sindicato das Agencias de Navegação Maritima do Estado de São Paulo)

SME *(small and medium enterprise*s)**:** small and medium-sized private businesses which conduct global trade.

SOLAS *(Safety of Life At Sea)*

SOPESP *(Port Operators Syndicate of the State of São Paulo)* (Sindicato dos Operadores Portuários do Estado de São Paulo)

SSPP (*Santos Port Security Plan) (*Sistema de Segurança Pública Portuária*)*: the first security plan jointly formed by CODESP and the University of São Paulo.

TAMP *(Tariff Authority for Major Ports)*: an independent authority established in 1997 to regulate all tariffs, both vessel and cargo related, as well as rates for lease of properties by MPT's and the private operators located therein.

TCA *(Tax and Customs Administration)*: the Netherlands' Customs organization.

TEU *(Twenty-foot-equivalent)*: a standard measurement for container capacity.

TWIC *(Transportation Workers ID Credential*): an international biometric identification program that is not yet fully implemented.

UCR *(Unique Consignment Reference)*: an alpha-numeric code, which includes numeric data components, short alpha country codes for where shipment originated an exporter identification number, and the exporter's internal reference number.

USCG *(United States Coast Guard)*

V&A *(The Victoria and Alfred Waterfront)*: a tourist attraction in South Africa with some port capabilities.

VACIS *(Vehicle and Cargo Inspection System)*: a component of SAIC's Integrated Container Inspection System, VACIS is a non-intrusive gamma ray imaging system for container trucks.

WCO *(World Customs Organization)*: an international organization that develops worldwide standards to facilitate the smooth movement of people and goods throughout the world.

WSC *(World Shipping Council):* a Council acting on behalf of ocean liners, representing their interests in the supply chain

WTO *(World Trade Organization):* an international organization that develops rules and standards for international commerce and provides mediation for trade disputes.

[1] International Maritime Organization, *International Ship and Port Facility Security (ISPS) Code and SOLAS Amendments 2002*, p. 3. Online. Available: http://www.turkloydu.org/EN/SEA/ISPS_Code_en.pdf#search=%22%20ISPS%20COde%22. Accessed: January 23, 2006.

[2] Ibid.

[3] Ibid.

[4] Waterfront Coalition, *Policy and Advocacy: Port Security Funding.* Online. Available: www.portmod.org?POLICY/policy.htm. Accessed: September 9, 2004.

[5] U.S. Department of Homeland Security, U.S. Customs and Border Protection, *C-TPAT Frequently Asked Questions*. Online. Available: http://www.Customs.ustreas.gov/xp/cgov/import/commercial_enforcement/ctpat/ctpat_faq.xml. Accessed: September 2, 2005.

[6] U.S. Customs and Border Protection. *CBP Factsheet*. Online. Available: www.customs.ustreas.gov/linkhandler/cgov/newsroom/fact_sheets/port_security/ctpat.ctt/ctpat.pdf. Accessed: May 23, 2006.

[7] U.S. Congress, Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Key Cargo Security Programs Can Be Improved*, 109th Congress, 1st session (May 26, 2005), GAO-05-466T, p. 2-4.

GAO, *Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, (March 2005, GAP-05-404), pp. 3-6.

[8] Keane, "Where's the Incentive?" p. 13.

[9] Peck, "Old, New Challenges for C-TPAT," p. 28.

[10] Kelly interview.

[11] Joseph Bonney, "A Good Use of Money," *Journal of Commerce*, June 6, 2005, p. 6.

[12] Courtney Tower, "WCO Trade Regime Faces Hurdles," (online).

[13] World Customs Organization (WCO), *The WCO Columbus Programme*, Brussels, Belgium (pamphlet).

[14] Kelly interview.

[15] U.S. Customs and Border Patrol, *About CBP.* Online. Available: http://www.cbp.gov/. Accessed: April 1, 2006.

[16] United States Coast Guard, *Coast Guard Fact File*. Online. Available: http://www.uscg.mil/USCG.shtm. Accessed: April 1, 2006.

[17] Ibid.

[18] U.S. Maritime Administration, *About MARAD*. Online. Available: http://www.marad.dot.gov/index.html. Accessed: April 1, 2006.

[19] Ibid.

[20] Ibid.

[21] Transportation Security Administration, *About TSA.* Online. Available: http://www.tsa.gov/public/. Accessed: April 1, 2006.

[22] Ibid

[23] Department of Homeland Security, *Fact Sheet: U.S. Customs and Border Protection's National Targeting Center.* Online. Available: http://www.dhs.gov/. Accessed: April 1, 2006.

[24] Bureau of Industry and Security (BIS). *Guiding Principles of the Bureau of Industry and Security*. Online. Available: http://www.bis.doc.gov/about/bisguidingprinciples.htm. Accessed: July 23, 2 006.
[25] Ibid.

[26] U.S. Customs and Border Patrol, *Acting Commissioner Spero Co-Chairs the Commercial Operations Advisory Committee (COAC)*. Online. Available: http://www.cbp.gov/. Accessed: April 1, 2006.

[27] http://www.aip.org/fyi/2006/076.html

[28] National Industrial Transportation League (NITL). *NITL Launches new Select Committee on Security*. Press Release (February 2005). Online. Available: http://www.nitl.org/press37.htm. Accessed: June 6, 2006.

[29] Ibid.

[30] Market Research.com. Alert. *Product Information.* Received via email on June 22, 2006. Also Available online: http://www.marketresearch.com/product/display.asp?productid=1264058&g=1.

[31] eWeek, *IBM plans GMM Supply Chain Security Initiative*. Online. Available: http://www.eweek.com/. Accessed: April 1, 2006.

[32] Siemens, *Prospering in a Secure Economy Executive Summary*. Online. Available: http://www.sbt.siemens.com/. Accessed: April 1, 2006.

[33] Haveman, Shatz and Vilchis, "U.S. Port Security Policy", p. 1.

[34] Ibid., p. 2.

[35] United States Coast Guard. *Maritime Transportation Security Act of 2002.* Online. Available: http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/MTSA2002.htm. Accessed: June 25, 2006.

[36] United States Coast Guard, *Coast Guard Fact File*. Online. Available: http://www.uscg.mil/USCG.shtm. Accessed: April 1, 2006.

[37] U.S. Customs and Border Protection. *Strategic Plan*. Online. Available: www.cbp.gov/.../cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf. Accessed: May 22, 2006.

[38] Investorwords.com, *Supply Chain Definition*. Online. Available: http://www.investorwords.com. Accessed: April 25, 2006.

[39] U.S. Customs and Border Protection, *Customs Trade Partnership Against Terrorism (CTPAT): Partnership to Secure the Supply Chain*. Online. Available: http://www.cbp.gov. Accessed: September 6, 2005.

[40] U.S. Customs and Border Patrol, *Keeping Cargo Safe: Container Security Initiative*. Online. Available: www.cbp.gov/. Accessed: April 1, 2006.

[41] Haveman, Shatz and Vilchis, "U.S. Port Security Policy", p. 4.

[42] U.S. Customs and Border Patrol, *Customs Today.* Online. Available: http://www.cbp.gov/. Accessed : April 1, 2006

[43] Haveman, Shatz and Vilchis, "U.S. Port Security Policy", p. 8.

[44] U.S. Customs and Border Patrol, *Customs Today.* Online. Available: http://www.cbp.gov/. Accessed : April 1, 2006

[45] U.S. Coast Guard, *96 Hour Notice of Arrival*. Online. Available: http:// www.uscg.mil/. Accessed: May 3, 2006.

[46] U.S. Department of Homeland Security (DHS). *Factsheet on Port Security.* Online. Available: http://www.dhs.gov/interweb/assetlibrary/DHSPortSecurityFactSheet-062104.pdf. Accessed: May 22, 2006.

[47] U.S. Customs and Border Patrol, *Automated Targeting System*, Online. Available: http://www.cbp.gov/. Accessed: April 1, 2006.

[48] U.S. Customs and Border Patrol, *ACE at a Glance.* Online. Available: http://www.cbp.gov/. Accessed: April 1, 2006.

[49] U.S. Customs and Border Patrol, *FAST Overview.* Online. Available: http//www.cbp.gov/. Accessed: April 1, 2006.

[50] TSA Moves Ahead with TWIC Card Proposals. Online. Available: http://www.all56.com/list0.php?docid=72937. Accessed July 26, 2006.

[51] Department of Homeland Security, *HSPDI13 Maritime Security Strategy.pdf*. Online. Available: http://www.dhs.gov/. Accessed: April 1, 2006.

[52] Ibid.

[53] U.S. Department of Transportation (DOT). "*DOT and Customs Launch 'Operation Safe Commerce' Program*." Online. Available: http://www.dot.gov/affairs/dot10302.htm. Accessed: June 22, 2006.

[54] SST Whitepaper. "*Smart and Secure Tradelanes*," (May 2003). Online. Available: http://www.savi.com/products/casestudies/wp.sst_initiative.pdf. Accessed: June 22, 2006.

[55] Ibid.

[56] U.S. Senator Patty Murray, *GreenLane Maritime Cargo Security Act*. Online. Available: http://murray.senate.gov/greenlane. Accessed: April 1, 2006.

[57] Ibid.

[58] U.S. House of Representatives Committee on Homeland Security, *Fact Sheet: The SAFE Port Act of 2006*. Online. Available: http://hsc.house.gov/SAFE_Port_Act_FactSheet_031206.pdf. Accessed: April 1, 2006.

[59] The National Industrial Transportation League, *The Notice Newsletter Volume 70.* Online. Available: http://www.nitl.org/publications.htm. Accessed: April 1, 2006.

[60] World Customs Organization, *About Us*. Online. Available: http://www.wcoomd.org/. Accessed: April 1, 2006.

[61] Ibid.

[62] Ibid.

[63] International Maritime Organization, *About IMO*. Online. Available: http://www.imo.org. Accessed: April 1, 2006.

[64] Ibid, (FAQ Page).

[65] Ibid.

[66] International Labour Organization. *About Us.* Online. Available: http://www.ilo.org/about.htm. Accessed: July 2, 2006.

[67] Eric Kulisch. "Tethering Cargo Security Standards." *American Shipper,* January 2006.

[68] International Organization for Standardization (ISO). *About ISO.* Online. Available: http://www.iso.org/iso/en/aboutiso/introduction/index.html#two. Accessed: June 25, 2006.

[69] American Shipper Article, Ibid.

[70] European Commission. "*Commission Proposes to Strengthen Security in European Ports*." Online. Available:

http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/212&format=HTML&aged=0&language=EN&guiLanguage=en. Accessed: May 22, 2006.

[71] Simon Heaney. "EC Security under Scrutiny," *American Shipper* (April 2006.)

[72] European Commission. *Taxation and Customs Union.* Online. Available: http://ec.europa.eu/taxation_customs/customs/policy_issues/international_customs_agreements/usa/index_en.htm. Accessed: May 24, 2006.

[73] Euractiv, *Transportation Security*. Online. Available: http://www.euractiv.com. Accessed: April 1, 2006.

[74] http://europa.eu.int/comm/taxation_customs/customs/policy_issues/. (online).

[75] Organization for Economic Cooperation and Development, *About OECD.* Online. Available: http://www.oecd.org. Accessed: April 1, 2006.

[76] Ibid.

[77] United Nations Conference on Trade and Development (UNCTAD). *About UNCTAD.* Online. Available: www.unctad.org. Accessed: June 22, 2006.

[78] National Academy of Sciences, Transportation Research Board: *Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment.* Online. Available: http://trb.org/mews/blurb_detail.asp?id=6277. Accessed: May 18, 2006.

[79] Asia-Pacific Economic Cooperation. *About APEC.* Online. Available: http://www.apecsec.org.sg/content/apec/about_apec/scope_of_work.html. Accessed: August 29, 2006.

[80] International Maritime Organization, *Introduction to the IMO*. Online. Available: http://www.imo.org. Accessed: April 1, 2006.

[81] International Organization for Standardization (ISO). *"ISO Offers Systematic Approach to Security Management in Global Supply Chains."* (November 2005). Online. Available: http://www.iso.org/iso/en/commcentre/pressreleases/archives/2005/Ref981.html. Accessed: August 2, 2006.

[82] International Organization for Standardization, *ISO/PAS 28000:2005*. Online. Available: http://www.iso.ch/iso/. Accessed: April 1, 2006.

[83] International Organization for Standardization, *ISO Offers Systematic Approach to Security Management in Global Supply Chains*. Online. Available: http://www.iso.ch/iso/. Accessed: April 1, 2006.

[84] International Federation of Customs Brokers Associations, *The Framework of Standards to Secure and Facilitate Global Trade*. Online. Available: http://www.ifcba.org. Accessed: April 1, 2006.

[85] World Customs Organization (WCO). *"Framework of Standards to Secure and Facilitate Global Trade."* Online. Available: http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/normes_WCO_en.pdf. Accessed: August 9, 2006.

[86] Ibid.

[87] Forbes, *Customs Framework will Transform Trade*. Online. Available: http://www.forbes.com. Accessed: April 1, 2006.

[88] Journal of Commerce, Supply-Chain Security, European Style. Online. Available: http://www.joc.com. Accessed: April 12, 2006.

[89] "Integrated Container Inspection System to Enhance Container Security and Expedite Traffic." *SAIC Security and Transportation Technology Whitepaper* (October 2004). Online. Available: http://www.saic.com/products/transportation/icis/ICIS_generic_white_paper_10-01a.pdf. Accessed: July 17, 2006.

[90] International Organization for Standardization (ISO). Online. Available: www.iso.ch/iso/en/commcentre/ isobulletin/articles/2003/pdf/ships03-06.pdf. Accessed: February 3, 2006.

[91] International Maritime Organization (IMO), *International Ship & Port Facility Security Code and SOLAS Amendments 2002* (London, 2003), p. 3-5.

[92] Congressional Research Service (CRS), "Port and Maritime Security: Background and Issues for Congress," report prepared by John Frittelli, Washington, D.C., May 20, 2003, p. 4.

[93] R.G. Edmonson, "On Course for July 1," *The Journal of Commerce*, (June 7-13, 2004) p. 15.

[94] IMO, *IMO Adopts Comprehensive Maritime Security Measures.* Online. Available: www.imo.org/Newsroom/mainframe.asp?topic_id=583&doc_id=2689. Accessed October 3, 2005.

[95] Ibid.

[96] IMO, *ISPS Code,* p. 3.

[97] National Industrial Transportation League (NTIL), *Coast Guard Finds Vessels Compliant*, (July 1, 2005) Online. Available: www.nitl.org. Accessed: July 2005.

[98] Fleet Inmarsat. Online. Available: http://fleet.inmarsat.com/F77_security.htm. Accessed: October 3, 2005.

[99] "Port Security and Maritime Transportation Security was Focus of Congressional Hearing." (July 22, 2005). Online. Available: http://www.tranzact.com. Accessed: July 22, 2005.

[100] U.S. House of Representatives, *The Subcommittee on Coast Guard and Maritime Trasnportation Hearing on Implementation of The Maritime Transportation Security Act.* Online. Available: http://www.house.gov/transportation/cgmt/06-09-04/06-09-04memo.html. Accessed: March 17, 2006.

[101] Ibid.

[102] Gordon Feller, "Singapore is Tracking Trucks and USCG Enforces ISPS," *Marine Digest and Cargo Business News, (*June 05) p. 26.

[103] IMO, *ISPS Code, p.* 8.

[104] Ibid., pp. 8-9.

[105] Ibid., pp. 12-13.

[106] Ibid., p. 15.

[107] Ibid., p. 18.

[108] Ibid., pp. 24-25.

[109] R.G. Edmonson, "July 1," p. 15.

[110] IMO, *ISPS Code,* p. 8.

[111] Ibid., p. 23.

[112] IMO, "IMO Adopts Comprehensive Maritime Security Measures." Online. Available: www.imo.org/Newsroom/mainframe.asp?topic_id=583&doc_id=2689. Accessed October 3, 2005.

[113] Ibid.

[114] Ibid.

[115] Ibid.

[116] "Port Security and Maritime Transportation Security." (July 22, 2005). Online. Available: http://www.tranzact.com. Accessed: March 30, 2006.

[117] U.S. Coast Guard. *Maritime Transportation Security Act of 2002.* Online. Available: http://www.uscg.mil/hq/g-m/mp/pdf/MTSA.pdf. Accessed: March 30, 2006.

[118] Coast Guard, Department of Homeland Security (DHS), 33 CFR *Navigation and Navigable Waters,* Chapter I, Subchapter H, *Maritime Security,* part 103.305, October 22, 2003.

[119] Ibid., 103.310.

[120] Ibid., 103.505.

[121] Ibid., 101.105.

[122] Ibid., 101.200.

[123] Ibid., 105.205(c).

[124] Ibid., 105.220.

[125] Ibid., 105.225.

[126] Ibid., 195.240.

[127] Ibid., 105.245.

[128] Ibid., 105.260.

[129] Ibid., 105.275.

[130] Ibid., 105.270.

[131] Ibid., 105.275.

[132] Ibid., 105.280.

[133] "Small Vessels, Big Security Risk" (July 6, 2005). Online. Available: www.lloydslist.com. Accessed: September, 2005.

[134] Ibid.

[135] Lloyd's Register-Fairplay, Ltd. The International Shipping Weekly, *A Day in the Life of … a Port Security Officer.* Available: www.fairplay.co.uk. Accessed: September 22, 2005.

[136] Lloyd's Register-Fairplay, Ltd. *A Day in the Life of … a Ship Security Officer.* Available: www.fairplay.co.uk. Accessed: September 22, 2005.

[137] Ibid.

[138] Ibid.

[139] Lloyd's Register-Fairplay, Ltd. *Maritime Security: ISPS-One Year on.* Online. Available: www.fairplay.co.uk. Accessed: September 22, 2005.

[140] Lloyd's Register-Fairplay, Ltd. *A Day in the Life of … a Ship Security Officer.* Online. Available: www.fairplay.co.uk.

[141] Ibid.

[142] Lloyd's Register-Fairplay, Ltd. *Maritime Security.* Online. Available: www.fairplay.co.uk. Accessed: September 22, 2005.

[143] Waterfront Coalition, *Policy and Advocacy: Port Security Funding.* Online. Available: www.portmod.org?POLICY/policy.htm. Accessed: September 9, 2004.

[144] Ibid.

[145] Ibid.

[146] CRS, "Port and Maritime Security," report prepared by John Frittelli, p. 16.

[147] Ibid., p. 16.

[148] Ibid.

[149] Ibid.

[150] Audience Discussion at Ship and Port Security Conference, Washington, D.C., January 30, 2006.

[151] Speech by Thomas Robison, Director of Transportation & Intermodal Security Division, Office of Domestic Preparedness, DHS, Maritime and Port Security Conference, Washington, D.C., January 30, 2006.

[152] R.G. Edmonson, "July 1," p. 15.

[153] R.G. Edmonson, "IMO Reports Higher Compliance." *The Journal of Commerce Online.* Online. Available: www.joc.com/20040614/sections/ocean/w50706.asp**.** Accessed: June 14, 2004.

[154] Marinelog, *USCG Port State Detentions Rise.* (June 13, 2005) Online. Available: www.marinelog.com/DOCS/NEWSMMV?2005jun012.html. Accessed: July, 5 2005.

[155] IMO. Online. Available: http://www.imo.org/home.asp. Accessed: March 30, 2006.

[156] Speech by Craig E. Bone, Director of Port Security, U.S. Coast Guard, DHS, Maritime and Port Security Conference, Washington, D.C., January 30, 2006.

[157] "Nossas finanças estão completamente no limite," *A Tribuna*, Santos, São Paulo, Sunday, June 4, 2006, p. A-17. Material comes from interview with financial director of Santos Port Authority, Mauro Marques.

[158] Lloyd's-Register Fairplay, Ltd. *Maritime Security.* Online.

[159] World Shipping Council (WSC). Online. Available: http://www.worldshipping.org/abo.html. Accessed: March 29, 2006.

[160] Eric Kulisch, "Tethering Cargo Security Standards," *American Shipper* (January 2006), p.23.

[161] Interview with Chris Koch, President and CEO, WSC, Washington, D.C., February 2, 2006.

[162] CRS, "Port and Maritime Security" report prepared by John Frittelli, p. 5.

[163] Ibid., p. 4.

[164] Speech by Craig E. Bone, January 30, 2006.

[165] Government Accountability Office (GAO). "Combating Terrorism, Actions Needed to Improve Force Protection for DoD Deployments Through Domestic Seaports," October, 2002.

[166] Smart Card Alliance. Online. Available: http://www.smartcardalliance.org/newsletter/May_2002.cfm. Accessed: March 30, 2006.

[167] Telephone interview with anonymous port official, March 2006.

[168] GAO. "Transportation Security, Post-September 11th Initiatives and Long-Term Challenges," report prepared by Gerald L. Dillingham, April 1, 2003.

[169] Koch interview.

[170] Speech by Craig Bone, Director of Port Security, U.S. Coast Guard, DHS to the Coast Guard and Maritime Transportation Subcommittee U.S. House of Representatives, June 29, 2005.

[171] Telephone interview with anonymous port official, March 2006.

[172] IMO, *ISPS Code*, p. iii

[173] U.S. Customs and Border Protection (CBP) *Recordkeeping Under the Mod Act.* Online. Available: http://www.cbp.gov/xp/cgov/import/informed_compliance/record_keeping.xml. Accessed on July 3, 2006.

[174] U.S. Customs and Border Protection (CBP), *Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan* (Washington, D.C., November 2004), p. 7.

[175] CBP, *C-TPAT Frequently Asked Questions*. Online. Available: http://www.customs.ustreas.gov/xp/cgov/import/commercial_enforcement/ctpat/ctpat_faq.xml. Accessed: September 2, 2005.

[176] UNCTAD Report by the Secretariat, Container Security: Major initiatives and related international developments, 26 February, 2004.

[177] *Securing the Global Supply Chain*, pp. 8, 18.

[178] Ibid., p. 8, 13-14, 25.

[179] Ibid., p. 8-9, 26-8.

[180] Ibid. pp. 9, 29-31.

[181] Ibid., p. 9, 32-4.

[182] *C-TPAT Frequently Asked Questions*. (online.)

[183] Office of Management and Budget (OMB). *DHS At a Glance*. Online. Available. www.whitehouse.gov/omb/budget/fy2006/dhs.html. Accessed July 2, 2006.

[184] Supply-Chain Security Update. JOC TPM Conference, March 7, 2006. (PowerPoint).

[185] UNCTAD Report by the Secretariat, Container Security: Major initiatives and related international developments, 26 February, 2004.

[186] Government Accountability Office (GAO), *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security (GAO-05-404)* (Washington, D.C., 2005), pp. 10-11.

[187] Ibid., p. 10-11.

[188] Ibid., p. 10-11.

[189] Ibid., p. 11-12.

[190] Crowley Maritime Corp., "Crowley Liner Service Earns Full Validation in U.S. Customs-Trade," *Seaports Press Review*, vol. 2, no. 15 (May 26, 2005), p. 1.

[191]U.S. Department of Homeland Security (DHS), CBP, *C-TPAT Importer Security Criteria*, (March 25, 2005). Online. Available: http://cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/criteria_importers/ctpat_importer_criteria.xml. Accessed: April 3, 2005.

[192]DHS, CBP, *C-TPAT Sea Carrier Security Criteria*, (March 1, 2006). Online. Available: http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/security_criteria/sea_carrier_criteria/sea_carrier_criteria.ctt/sea_carrier_criteria.doc. Accessed: April 3, 2005.

[193]DHS, CBP, *C-TPAT Highway Carrier Security Criteria*, (March 13, 2006). Online. Available: http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/security_criteria/hwy_carrier_criteria/hwy_carrier_criteria.xml. Accessed: April 3, 2005.

[194] U.S. Congress, Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Key Cargo Security Programs Can Be Improved*, 109th Congress, 1st session (May 26, 2005), GAO-05-466T, p. 2-4.

GAO, *Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, (March 2005, GAP-05-404), pp. 3-6.

[195] Angela Greiling Keane, "Security in the GreenLane?" *Traffic World* (January 24, 2005), p. 12.

[196] Angela Greiling Keane, "Where's the Incentive?" *Traffic World* (April 11, 2005), p. 13.

[197] R.G. Edmonson, "An Idea Whose Time Has (Almost) Come," *The Journal of Commerce* (February 28, 2005), p. 43.

[198] William G. "Jerry" Peck, "Old, New Challenges for C-TPAT," *The Journal of Commerce* (February 14, 2005), p. 28.

[199] Keane, "Where's the Incentive?" p. 13.

[200] Peck, "Old, New Challenges for C-TPAT," p. 28.

[201] R.G. Edmonson, "Grand Design," *The Journal of Commerce* (November 7, 2005), p. 21.

[202] Keane, "Security in the GreenLane?" p. 12.

[203] Lyndon B. Johnson School of Public Affairs, Survey of National Industry of Transportation League Members, March 2006.

[204] Eric Kulisch. "COAC Proposes GreenLane Benefits." *American Shipper*, January 2006.

[205] Ibid.

[206] Eric Kulisch. "Beyond the GreenLane." *American Shipper*, November 2005.

[207] The National Industrial Transportation League (NITL), "House Port Security Bill on Fast Track," *Notice*, Vol. 7 (March 17, 2006), p. 1.

[208] U.S. Library of Congress. THOMAS Home. *Window on H.R. 4954.* Online. Available: http://thomas.loc.gov/cgi-bin/thomas. Accessed: July 7, 2006.

[209] Ibid., p. 1-2.

[210] http://thomas.loc.gov/cgi-bin/thomas. Online. Window on H.R. 4954. Accessed July 7, 2006.

[211] W. Scott Gould and Christian Beckner, "*Global Movement Management: Securing the Global Economy*," (IBM Global Leadership Initiative, September 2005). p. 1

[212] Ibid., p. 24.

[213] Ibid., p. 3.

[214] Ibid., p. 7.

[215] Presentation by Jozef Hupperetz, European Commission, Taxation and Customs Union Directorate-General, Miami, April 21, 2005.

[216] European Commission (EC), Taxation and Customs Union, "Customs 2007 Project/pilot action, Authorised Economic Operators, Operator's Guidelines on Standards and Criteria," January 2006.

[217] Presentation by Jozef Hupperetz, EC, Taxation and Customs Union Directorate-General, Miami, April 21, 2005.

[218] EC, Taxation and Customs Union, "The Authorised Economic Operator," January 2006.

[219] Interview by Renee Leta with Joe Kelly, Colombus Programme Manager, Customs Modernization Capacity Building, Capacity Building Directorate, World Customs Organization, Brussels, Belgium, February 3, 2006.

[220] World Customs Organization (WCO), *Fact Sheet - World Customs Organization.* Online. Available: http://www.wcoomd.org/ie/En/AboutUs/aboutus.html. Accessed: April 10, 2006.

[221] "WCO Framework of Standards to Secure and Facilitate Global Trade," *WCO News*, no. 3 (October 2005), pp.30-31.

[222] http://www.wcoomd.org/ie/En/AboutUs/aboutus.html

[223] Ibid.

[224] Ibid.

[225] Interview by Renee Leta with Robert Ireland, Technical Attache, Capacity Building Directorate, World Customs Organization, Brussels, Belgium, February 7, 2006.

[226] World Customs Organization (WCO), *WCO Brochure,* Online. Available: http://www.wcoomd.org/ie/En/AboutUs/aboutus.html. Accessed: April 10, 2006

[227] Kelly interview

[228] WCO, *Fact Sheet – World Customs Organization,* (online).

[229] Ibid.

[230] Ibid.

[231] WCO Brochure, Online.

[232] Ibid.

[233] Ibid.

[234] Kelly interview.

[235] Ibid.

[236] Email from Robert Ireland, Director of Capacity Building at the WCO to Jacqueline Carton, June 30, 2006.

[237] Kelly interview.

[238] Kelly interview.

[239] Courtney Tower, "WCO Trade Regime Faces Hurdles," *Journal of Commerce Online*. Online. Available: http://www.joc.com/20050513/sections/edit/w80375.asp. Accessed: April 10, 2006.

[240] Kelly interview.

[241] "WCO Framework of Standards to Secure and Facilitate Global Trade," *WCO News*, no. 3 (October 2005), pp.30-31.

[242] Ibid.

[243] "WCO develops a Framework of Standards to Secure and Facilitate Global Trade," *WCO Press Release,* December 9, 2004.

[244] "WCO Framework of Standards to Secure and Facilitate Global Trade," *WCO News*, pp.30-31.

[245] Courtney Tower, "WCO Trade Regime Faces Hurdles," (online).

[246] "WCO Framework of Standards to Secure and Facilitate Global Trade," *WCO News*, pp.30-31.

[247] "US Joins New WCO Standards," *NITL Notice*, July 1, 2005, pp. 3-4.

[248] Ibid.

[249] Joseph Bonney, "A Good Use of Money," *Journal of Commerce*, June 6, 2005, p. 6.

[250] Hironori Asakura, World History of the Customs and Tariffs (Brussels: World Customs Organization, 2003).

[251] Interview by Renee Leta with Stefan Bjorkencrona, National Expert, and Jozef Hupperetz, Supply Chain Security, Taxation and Customs Union Directorate-General, European Commission, Brussels, Belgium, February 7, 2005.

[252] Ibid.

[253] Ireland interview.

[254] International Federation of Customs Brokers Associations. Online. Available: http://www.ifcba.org/modules/news/article.php?storyid=142. Accessed on June 18, 2006.

[255] Courtney Tower, "WCO Trade Regime Faces Hurdles," (online).

[256] "WCO develops a Framework of Standards to Secure and Facilitate Global Trade," *WCO Press Release,* December 9, 2004.

[257] Email from Robert Ireland, Director of Capacity Building at the WCO to Jacqueline Carton, July 25, 2006.

[258] Ibid.

[259] Chris Gillis and Eric Kulish, "Going Global with Security," *American Shipper*, January, 2006, pp. 36-40.

[260] Ibid.

[261] Kelly interview.

[262] Ibid.

[263] Ibid.

[264] World Customs Organization (WCO), *The WCO Columbus Programme*, Brussels, Belgium (pamphlet).

[265] World Customs Organization (WCO), *The WCO Columbus Programme*.

[266] Email from ShippersNewsWire@americanshipper.com, "Customs authorities endorse supply chain security regime," to Leigh Boske, June 24, 2005.

[267] R.G. Edmonson, "Challenges Remain for World Security and Trade System," pp.58-59.

[268] Email from ShippersNewsWire@americanshipper.com, "U.S. ready to commit $20 million to WCO cargo security effort," to Leigh Boske, June, 23, 2005.

[269] Ibid.

[270] R.G. Edmonson, "Challenges Remain for World Security and Trade System," pp.58-59.

[271] Philip Damas, "Global Security Controls on Supply Chain," *American Shipper*, August, 2003, pp. 20-26.

[272] R.G. Edmonson, "Grand Design" *Journal of Commerce*, November 7, 2005, pp. 20-21.

[273] Ibid.

[274] Ireland interview.

[275] Kelly interview.

[276] Ibid.

[277] Ibid.

[278] Kelly interview.

[279] Ibid.

[280] Ibid.

[281] R.G. Edmonson, "Challenges Remain for World Security and Trade System," pp.58-59.

[282] Chris Gillis and Eric Kulish, "Going Global with Security," pp.36-40.

[283] Kelly interview.

[284] Ibid.

[285] Ibid.

[286] Ireland interview.

[287] Ibid.

[288] Karen Brooks, "How to Deliver the WCO Framework," *Journal of Commerce*, December 19, 2005, p. 32.

[289] Ibid.

[290] Kelly interview.

[291] Kelly interview.

[292] Ibid.

[293] Central Intelligence Agency, "Brazil", *The World Factbook*. Online. Available: http://www.cia.gov/cia/publications/factbook/print/br.html. Accessed May 14, 2006.

[294] *CIA World Factbook.*

[295] Ibid.

[296] *Brazilian Trade Balance-Consolidated Data*, Ministry of Development, Industry and Foreign Trade, Brasília, DF, 2006.

[297] Ministry of Justice, Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CONPORTOS). Online. Available: http://www.mj.gov.br/senasp/conportos/. Accessed: May 4, 2006.

[298] Ministry of Justice, *Plano Nacional de Segurança Portuária*, Brasília, DF, December 2002, p. 9.

[299] Ibid., p. 19.

[300] Ibid., p. 10.

[301] Ibid., pp. 11-13.

[302] Ibid., pp. 14-16.

[303] Ministry of Development, Industry and Foreign Trade, CAMEX. Online. Available: http://www.mdic.gov.br. Accessed December 12, 2005.

[304] Ibid.

[305] Interview with Rodrigo Pierdominici, Commercial Director, Port Authority of Santos, Santos, Brazil, May 15, 2006 and "Reporto beneficia novos investimentos no Porto de Santos," NetMarinha online, June 10, 2005. Online. Available: http://www.netmarinha.com.br. Accessed: May 16, 2006.

[306] Port of Santos, *Relatório da Administração e Demonstrações Contabeis 2005* (Port of Santos Annual Report 2005). Online. Available: www.portodesantos.com.br. Accessed: May 1, 2006, p. 4.

[307] Ibid.

[308] National Waterborne Transport Agency (Agência Nacional de Transportes Aquaviária, ANTAQ), "Porto de Santos." Online. Available: www.antaq.gov.br/PortalPortos/EstudosRelatorios/Anuario2004/Portos/Santos.htm. Accessed: May 14, 2006.

[309] Port of Santos Annual Report 2005, p. 10.

[310] Ibid., p. 11.

[311] Ibid.

[312] CONPORTOS Resolution No. 22, March 5, 2004.

[313] Ibid.

[314] CONPORTOS Resolution No. 18-19, Dec. 18, 2003.

[315] CONPORTOS Resolution No. 14, Dec. 17, 2003.

[316] Ministry of Justice, CONPORTOS, *Instalações Portuárias-Quadro Geral*, March 20, 2006. Online. Available: http://www.mj.gov.br/senasp/conportos/. Accessed: May 4, 2006.

[317] "Nossas finanças estão completamente no limite," *A Tribuna*, Santos, São Paulo, Sunday, June 4, 2006, p. A-17. Material comes from interview with financial director of Santos Port Authority, Mauro Marques.

[318] Ibid. pp. A-17-A-18.

[319] Port of Santos Annual Report, p. 16.

[320] Fundação de Apoio à Universidade de São Paulo (FUSP), *Sistema de Segurança Pública Portuária-Fase I: Cartilha de Controle de Acesso nas Áreas Restritas do Porto de Santos* , São Paulo, SP, September 19, 2005.

[321] FUSP, *Sistema de Segurança Pública Portuária-Fase I: Cartilha de Controle de Acesso nas Áreas Restritas do Porto de Santos* , São Paulo, SP, September 19, 2005, pp. 2-3.

[322] Interview with Eng. Alvaro Luiz Dias Oliveira, Security Officer, Companhia das Docas do Estado de São Paulo (CODESP), at Floripa Trade Summit, Florianópolis, Santa Catarina, April 6, 2006.

[323] "CODESP inicia controle de acesso eletrônico em sua sede," *A Tribuna* Online , Santos, São Paulo, April 18, 2006. Online. Available: atribunadigital.globo.com/bn_print.asp?cod=243130&opr=82. Accessed: May 4, 2006.

[324] Email from Eng. Alvaro Luiz Dias Oliveira, Security Officer, CODESP, to John Cuttino, May 5, 2006.

[325] Email alert from ISPS Santos (www.ispssantos.com.br) to John Cuttino, April 19, 2006, citing article "Apupesp fará mutirão para novas crachás, *A Tribuna* Digital, Santos, São Paulo.

[326] "Codigo de segurança cria mais custos nos portos," cited at www.portosenavios.com.br., September 20, 2005.

[327] "Container Security Initiative Port of Santos, Brazil Is Targeting and Pre-Screening Cargo Destined for U.S.," U.S. Customs and Border Protection press release, Washington D.C,., Sept. 22, 2005, U.S. Customs and Border Protection website. Online. Available: www.cbp.gov. Accessed June 5, 2006.

[328] Ministry of Justice, Segurança Online, "Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis-CONPORTOS." Online. Available: www.mj.gov.br/senasp/conportos/conselhos_conp_situa.htm. Accessed: May 4, 2006.

[329] "Customs Mutual Assistance Agreements (CMAA) by Country," U.S. Customs and Border Protection. Online. Available: http:www.cbp.gov/xp/cgov/border_security/international_activities/international_agreements. Accessed: May 14, 2006.

[330] Central Intelligence Agency (CIA), *CIA-The World Factbook* (Washington, D.C.: March 2006). Available: http://www.cia.gov/cia/publications/factbook/index.html. Accessed March 03, 2006.

[331] Ministère des Transports, de l'Equipement du Tourisme et de la Mer (MTETM), *Window on French Ports and Organizational Structure.* Online. Availabe: http://mer.equipement.gouv.fr. Accessed: November 21, 2005.

[332] United Nations (UN), *Window on Maritime Legislation and Treaties.* Online. Available: http://www.un.org/Depts/los/legislationandtreaties. Accessed: January 21, 2006.

[333] European Sea Ports Organization (ESPO), *Factual Report on the Port Sector* (March 2005). Online. Available: http://www.espo.be/downloads/archive/dac5f5da-3b43-4cce-a661-9d1c4c2369a4.pdf: Accessed: March 6, 2006.

[334] Interview by Jacqueline Carton with Jean-Pierre Marcorelles, President, Association des Transitaires Organisateurs de Transports Multimodaux (Association of Organizing Freight Forwarders of Multimodal Shipments) , Marseille, France, March 13, 2006.

[335] European Sea Ports Organization (ESPO), *Annual Report 2005* (February 2006). Online. Available: http://www.espo.be/downloads/archive/6fc09ed1-d06f-423d-8b0d-11b490d88ecb.pdf: Accessed: March 6, 2006.

[336] Port Authority of Le Havre (PAH), *Window on Organization of the Port.* Online. Available: http://www.havre-port.net. Accessed: January 19, 2006.

[337] Office International de l'Eau (International Office of Water), *French Water Act of January 3, 1992, Article 4*", Journal Officiel" Jan. 4, 1992, p. 187

[338] Ibid.

[339] European Sea Ports Organization (ESPO), *Annual Report 2004* (February 2005). Online. Available: http://www.espo.be/downloads/archive/944663af-2af9-487f-ad04-a08d096f4e26.pdf: Accessed: March 6, 2006.

[340] MTETM, *Window on French Ports and Organizational Structure.* Online.

[341] Ministère de l'Economie, des Finances et de l'Industrie - La Douane (MEFID), *Window on Customs Training.* Online. Available: http://www.douane.gouv.fr/organization

[342] Ministère de l'Economie, des Finances et de l'Industrie - La Douane (MEFID), Customs Service Annual Report 2005 (January 2006). Online. Available: http://www.douane.gouv.fr/pdf/actualite/resultats05.pdf

[343] Ministère de l'Economie, des Finances et de l'Industrie - La Douane (MEFID), *Window on French Customs Code, Section 60.* Online. Available: http://www.douane.gouv.fr. Accessed: February 26, 2006.

[344] Ibid., Section 61.

[345] Ibid., Section 63b.

[346] MEFID , *French Customs Code*, Section 64.

[347] Ibid., Section 65.

[348] Ibid., Section 413a.

[349] Ibid., Section 67a.

[350] Ibid., Section 44a.

[351] Ibid., Section 62.

[352] Ibid., Section 63.

[353] Ibid., Section 16, Act 94-589.

[354] Ibid., Section 25a (25 bis), Act 90-614.

[355] Ibid., Section 67c.

[356] Ibid., Section 67b.

[357] "Customs and Excise Service Powers," Embassy of France in the United States, October 10, 2001 (press release).

[358] Lloyd's Register-Fairplay, Ltd. *Ports and Terminals Guide*. Online. Accessible: http://www.portguide.com. Accessed: February 1, 2006.

[359]Port Authority of Marseille (PAM), *Window on Port History.* Online. Available: http://www.marseille-port.fr. Accessed: January 22, 2006.

[360] Lloyd's Register-Fairplay, Ltd. *Ports and Terminals Guide*. (Online).

[361] Port Authority of Marseille (PAM), *Window on Reporter Magazine.* Online. Available: http://www.marseille-port.fr. Accessed: January 22, 2006.

[362] Interview by Jacqueline Carton with Guy Janin, Port Director, and Joseph Moysan, Port Commander, Port Authority of Marseille, Marseille, France, March 15, 2006.

[363] Janin & Moysan interview.

[364] Ibid.

[365] Online. Available: www.premier-ministre.gouv.fr/information/ fiches_52/plan_vigipirate_50932.html. Accessed June 14, 2006.

[366] "Port Security Raised to Red," Port Authority of Marseille, July 15, 2005 (press release).

[367] Janin & Moysan interview.

[368] Interview by Jacqueline Carton with Marc Reverchon, President, Maritime and Fluvial Union, and Jean-François Mahé, Director of Container Logistics and Security, CMA-CGM, Marseille, France, March 14, 2006.

[369] Vaccà interview.

[370] Ibid.

[371] Ibid.

[372] Ibid.

[373] Interview by Jacqueline Carton with Francois Brivet, Co-Director of Regional Customs for Marseille, Marseille, France, March 14, 2006.

[374] Ibid.

[375] Brivet interview.

[376] Ibid.

[377] Ibid.

[378] Janin & Moysan interview.

[379] Central Intelligence Agency, *CIA World Factbook.* Online. Available: http://www.cia.gov/cia/publications/factbook/index.html. Accessed: March 31, 2006.

[380] Grand Power Logistics Group Inc., Hong Kong, January 2006 (PowerPoint).

[381] Lloyd's Register-Fairplay, Ltd. *Ports and Terminals Guide*. Online. Accessible: http://www.portguide.com. Accessed: April 1, 2006.

[382] Ibid.

[383] Central Intelligence Agency, *CIA World Factbook* (online).

[384] Lloyd's Register-Fairplay, Ltd. *Ports and Terminals Guide*. (online).

[385] Hong Kong Port Development Council, *Home*. Online. Available: http://www.pdc.gov.hk/eng/home/index.htm. Accessed: January 2, 2006.

[386] Hong Kong Marine Department, *Hong Kong: The Facts*. Online. Available: http://www.mardep.gov/hk/thefacts. Accessed: March, 25, 2006.

[387] Ibid.

[388] Ibid.

[389] Lloyd's Register-Fairplay, Ltd. *Ports and Terminals Guide*. (online).

[390] Modern Terminals, LTD. Online. Available: http://www.modernterminals.com. Accessed: March 31, 2006.

[391] DP World, *Home*. Online. Available: http://www.dpworld.com. Accessed: April 2, 2006.

[392] Hutchison International Terminals, *About HIT*. Online. Available: http://www.hit.com.hk/aboutHIT/co_profile.html. Accessed: March 30, 2006.

[393] Ibid.

[394] Lloyd's Register-Fairplay, Ltd. *Ports and Terminals Guide*. (online).

[395] Hutchison International Terminals, *About HIT*. (online).

[396] Hutchison Port Holdings, *River Trade Terminal*. Online. Available: http://www.hph.com.hk/business/ports/hong_kong/rtt.htm. Accessed: March 31, 2006.

[397] Hong Kong Trade Development Council, *Economic and Trade Information on Hong Kong*. Online. Available: http://www.dtctrade.com/main/economic.htm. Accessed: April 2, 2006.

[398] U.S. Department of State, Bureau of East Asian and Pacific Affairs. Online. Available: http://www.state.gov/r/pa/ei/bgn/2747.htm. Accessed: March 24, 2006.

[399] Hong Kong Port Development Council, *Window on Hong Kong Port Facilities*. (online).

[400] Lloyd's Register-Fairplay, Ltd. *Ports and Terminals Guide*. (online).

[401] Telephone interview by Lindsey Ford with John Kok, General Manager – CSI, Hutchison Port Holdings, Hong Kong SAR, China; George Chu, Hutchison Port Holdings; and Paul Ho, Port Facility Security Officer, Hutchison International Terminals, Hong Kong SAR, China, March 21, 2006.

[402] Hutchison Port Holdings, *Window on Asia Port Services*. (online).

[403] Lloyd's Register-Fairplay, Ltd. *Ports and Terminals Guide*. (online).

[404] Hong Kong Marine Department, *About Us*. (online).

[405] Hong Kong Economic Development and Labour Bureau, *Port, Maritime and Logistics Services*. Online. Available: http://www.edlb.gov.hk/edb/eng/resp/port.htm. Accessed: March 31, 2006.

[406] The Government of the Hong Kong Special Administrative Region of the People's Republic of China, *Organization Chart*. Online. Available: http://www.info.gov.hk/govcht_e.htm. Accessed: March 25, 2006.

[407] Hong Kong Marine Department, *Organization, Functions and Services*. (online).

[408] Ibid.

[409] Ibid.

[410] Ibid.

[411] Ibid.

[412] Ibid.

[413] Ibid.

[414] Ibid.

[415] Hong Kong Economic and Trade Office, London, *About Us*. Online. Available: http://www.hketolondon.gov.hk/about/respon.htm. Accessed: March 25, 2006.

[416] Hong Kong Port Development Council, *About Us*. (online).

[417] Hong Kong Economic Development and Labour Bureau, *Port, Maritime and Logistics Services*. (online).

[418] Hong Kong Police Force, Superintendent C.J. Wilson, "Briefing for DVCs with PF Responsibilities on International Shipping and Port Facility Security Code," Hong Kong SAR, China (PowerPoint).

[419] Email from W.H. Wong, Senior Marine Officer, Hong Kong Marine Department. "Re: University of Texas Research Project" to Lindsey Ford, February 20, 2006.

[420] Hong Kong Marine Department, *Minutes of the 4th Port Area Security Advisory Committee* (May 13, 2004). (online).

[421]W.H. Wong email.

[422] Hong Kong Police Force, Superintendent C.J. Wilson, "International Ship and Port Facility (ISPS) Code Brief – Line To Take and Q&As," Hong Kong SAR, China (briefing document).

[423] Email from Henry Lee, Executive Director, Hong Kong Container Terminal Operators Association. "Re: Request for Mr. Henry Lee," to Lindsey Ford, March 9, 2006.

[424] Kok et al. telephone interview.

[425] Ibid.

[426] Hong Kong Marine Department, *Port Area Security Advisory Committee*. (online).

[427] Ibid.

[428] Hong Kong Marine Department, *Minutes of the 2nd Port Area Security Advisory Committee* (September 17, 2003). (online).

[429] Ibid.

[430] Kok et al. telephone interview.

[431] Interview by Lindsey Ford with C.J. Wilson, Superintendent of Police DVC KTDIV, Hong Kong SAR, China, January 12, 2006.

[432] Hong Kong Security Bureau, *Boundary Control*. Online. Available: http://www.sb.gov.hk/eng/special/bound/control.htm. Accessed: April 2, 2006.

[433] Ibid.

[434] Ibid.

[435] Ibid.

[436] Hong Kong Container Terminal Operators Association. Online. Available: http://www.hkctoa.com/. Accessed: November 14, 2005.

[437] Telephone interview by Lindsey Ford with John Kok, General Manager – CSI, Hutchison Port Holdings, Hong Kong SAR, China, February 22, 2006.

[438] Ibid.

[439] Ibid.

[440] Hong Kong Container Terminal Operators Association, *What's New*. (online).

[441] Science Applications International Corporation, *Products: Integrated Container Inspection System. Online*. Available: http://www.saic.com/products/transportation/icis. Accessed: October 21, 2005.

[442] Kok et al. telephone interview.

[443] Hong Kong Container Terminal Operators Association, *What's New*. (online).

[444] Kok et al. telephone interview.

[445] Ibid.

[446] Science Applications International Corporation, *Products: Integrated Container Inspection System*. (online).

[447] Ibid.

[448] Kok et al. telephone interview.

[449] Hong Kong Container Terminal Operators Association, *What's New*. (online).

[450] John Kok telephone interview.

[451] Ibid.

[452] Hong Kong Marine Department, *Merchant Shipping (Security of Ships and Port Facilities) Ordinance*, CAP 582, Section 6(2)j (June 29, 2004). Online. Available: http://www.mardep.gov.hk/en/publication/home.html. Accessed: November 14, 2005.

[453] Hong Kong Marine Department, *Merchant Shipping (Security of Ships and Port Facilities) Ordinance*, CAP 582A, Section 9(2) and CAP 582A, Section 24(2). (online).

[454] Ibid.

[455] Ibid.

[456] Ibid.

[457] Hong Kong Marine Department, *Minutes of the 3rd Port Area Security Advisory Committee* (December 19, 2003). (online).

[458] Ibid.

[459] Hong Kong Police Force, "Briefing for DVCs" (PowerPoint).

[460] Ibid.

[461] Kok et al. telephone interview.

[462] Hong Kong Police Force, "Briefing for DVCs" (PowerPoint).

[463] Ibid.

[464] W.H. Wong email.

[465] The Government of the Hong Kong Special Administrative Region of the People's Republic of China, *The Basic Law*, (April 4, 1990). Online. Available: http://www.info.gov.hk/basic_law/fulltext/. Accessed: April 1, 2006.

[466] The Government of the Hong Kong Special Administrative Region of the People's Republic of China, *Organization Chart*. (online).

[467] Hong Kong Customs and Excise Department, *Vision, Mission and Values*. Online. Available: http://www.customs.gov.hk/eng/about_vision_e.html. Accessed: April 1, 2006.

[468] Hong Kong Customs and Excise Department, *About Us*. (online).

[469] Ibid. The Boundary and Ports Branch is headed by Assistant Commissioner Mr. Kwong Chow.

[470] Hong Kong Customs and Excise Department, *Hong Kong: The Facts*. (online).

[471] Hong Kong Customs and Excise Department, *Import/Export Clearance*. (online).

[472] Ibid.

[473] Ibid.

[474] Alan M. Field, "No place for beginners," *The Journal of Commerce* (May 30, 2005), p. 6A.

[475] Ibid.

[476] Modern Terminals LTD, *News Flash*. (online).

[477] Ibid.

[478] Hong Kong Trade Development Council, *Business Alert – US*. (online).

[479] Hong Kong Customs and Excise Department, *World Customs Organization Framework of Standards to Secure and Facilitate Global Trade and Asia Pacific Economic Cooperation Framework for Secure Trade*, working paper (November 2005). Online. Available: http://www.haffa.com.hk/rs.html. Accessed: March 31, 2006.

[480] Hutchison International Terminals, *Press Release* (February 24, 2003). (online).

[481] Ibid.

[482] Kok et al. telephone interview.

[1] CIA World Factbook. Online, Available: http://www.odci.gov/cia/publications/factbook/geos/in.html. Accessed: February 17, 2006.

[484] Government of India (GOI), Department of Shipping (DOS), Online. Available: http://shipping.nic.in/Org[1].history.htm. Accessed: March 30, 2006.

[485] (GOI), (DOS), Online. Available: http://shipping.nic.in/subjects.htm. Accessed: March 30, 2006.

[486] (GOI) Press Information Bureau. "India Observes Maritime Day" Online. Available: http://pib.nic.in/feature/feyr2001/fmar2001/f260320011.html. Accessed: June 18, 2006.

[487] (GOI), (DOS), Autonomous Bodies: Chennai Port Trust, Cochin Port Trust, Jawaharlal Nehru Port Trust, Kandla Port Trust, Kolkata Port Trust, Mormugao Port Trust, Mumbai Port Trust, New Mangalore Port Trust, Paradip Port Trust, Tuticorin Port Trust, Visakhapatnam Port Trust. Online. Available: http://shipping.nic.in/. Accessed: March 24, 2006.

[488] Committee on Infrastructure, *Ports*. Online. Available: http://infrastructure.gov.in/port.htm. Accessed: June 29, 2006.

[489] (GOI), (MPTA), Chapter II: *Board of Trustees & Committees Thereof,* 1963. Online. Available: http://www.indialawinfo.com/bareacts/mpta.html#_Toc498334089. Accessed: March 30, 2006.

[490] (GOI), Tariff Authority for Major Ports (TAMP). Online. Available http://tariffauthority.gov.in/ Accessed: March 31, 2006.

[491] Ray, Amit, *Managing Port Reforms in India: Case Study of The Jawaharlal Nehru Port Trust.* University of Jawaharlal Nehru: (Background Paper Prepared for the World Development Report). February, 2004. p.10

[492] (GOI), (DOS). (Online).

[493] (GOI), (DOS). (Online).

[494] Ray, Amit, "*Managing Port Reforms in India,"* p.9

[495] Ibid.

[496] (GOI), Consitution of India. Part XI, Seventh Schedule. Online. Available: http://www.constitution.org/cons/india/p11.html Accessed: March 24, 2006.

[497] (GOI), The Minsistry of Home Affairs, *Window on Role*. Online. Available: http://mha.nic.in/mini.htm#Role%20of%20Ministry%20of%20Home%20Affairs. Accessed February 2, 2006.

[498] (GOI), The Central Industrial Security Force Act(CISF Act), *No.50 of 1968*, (March 10,1969. As modified vide Act No.14 of 1983,
20 of 1989 and 40 of 1999). Online. Available: http://cisf.nic.in/eng_ver.htm. Accessed: February 2, 2006.

[499] (GOI), The Central Industrial Security Force. Online. Available: http://cisf.nic.in/zonewise.htm. Accessed: February 9, 2006.

[500] (GOI), The Central Industrial Security Force. (Online).

[501] (GOI), The Central Industrial Security Force (CISF). (Online).

[502] (GOI), *The CISF Act, 1968, Section 2 (B).* (Online).

[503] (GOI), (CISF). (Online).

[504] (GOI) *The CISF Act 1968, No.50,* (Online).

[505] (GOI), (CISF). (Online).

[506] GlobalSecurity.org., *Military: The Central Industrial Security Force.* Online. Available: http://www.globalsecurity.org/military/world/india/cisf.htm. Accessed: February 2, 2006.

[507] Ibid

[508] (GOI), Ministry of Home Affairs: *National Security Guard,* Online. Available: http://mha.nic.in/nsg.htm. Accessed: January, 18, 2006.

[509] (GOI), Central Board of Excise & Customs (CBEC), Online. Available: http://www.cbec.gov.in/cae/whoweare/whoweare.htm. Accessed: February, 7, 2006.

[510] (GOI) (CBEC), *Window on Strategies 1-6.* (Online).

[511] (GOI) (CBEC), *Index of Customs Act, 1962.* (Online).

[512] Ray, Amit, "*Managing Port Reforms in India,"* p. 12

[513] Lloyd's Register-Fairplay, Ltd. *Ports & Terminals Guide*, CDROM: 2006 Edition. Jawaharlal Nehru Port. India. Accessed: March 28, 2006.

[514] JNPT Port. *Productivity at JNPT Crosses 100 Moves Per Hour Mark.* March 2nd 2006. Online. Available: http://www.jnport.com/new_site/news_pressrelease.asp. Accessed: March, 28, 2006

[515] Interview by Ben Stark with Captain Jitendra Mishra, Deputy Conservator, Jawaharlal Nehru Port Trust, Mumbai India, January 13, 2006.

[516] JNPT Port. *New Container Terminal*. Online. Available: http://www.jnport.com/new_site/facilities_newcontainerterminal.asp. Accessed: February, 25, 2006.

[517] Ibid.

[518] Ray, Amit, "*Managing Port Reforms in India,"* p. 24

[519] NSICT Terminal. Online. Available: http://portal.pohub.com/portal/page?_pageid=147,149089,147_149221:147_149253&_dad=pogprtl&_schema=POGPRTL. Accessed: March 22, 2006

[520] Ibid.

[521] Ray, Amit, "*Managing Port Reforms in India,"*, p. 17

[522] Lloyd's Register-Fairplay, Ltd. *Ports & Terminals Guide*. (CD ROM) 2006. Accessed: March 28, 2006.

[523] Mishra interview.

[524] Ibid.

[525] Ibid.

[526] Ibid.

[527] Ibid.

[528] Ibid.

[529] Singh & Munjal interview.

[530] Consolidated information about both terminals revealed during separate interviews by Ben Stark with Capt. Mishra, January 12, 2006 and Singh & Munjal, January 10, 2006. (Mishra et. al interviews).

[531] Mishra, et al. interviews.

[532] Ibid.

[533] Interview by Ben Stark with Captain Sujeet Singh, General Manager, Operations, & Capt. Girish J. Munjal, Manager Security & Training, at NSICT Terminal, JNPT, Mumbai, India, January 10, 2006.

[534] Sing & Munjal interview.

[535] Mishra interview.

[536] Mishra interview.

[537] Mishra et al. interviews.

[538] Mishra interview.

[539] Singh & Munjal interview.

[540] Mishra interview.

[541] Singh & Munjal interview.

[542] Mishra interview.

[543] Singh & Munjal interview.

[544] Singh & Munjal interview.

[545] Mishra interview.

[546] Singh & Munjal interview.

[547] Interview by Ben Stark with S.A. Usmani, Joint Commissioner, Jawaharlal Nehru Custom House, Sheva, Mumbai India,. January 12, 2006.

[548] Usmani interview.

[549] Usmani interview.

[550] Ibid.

[551] Ibid.

[552] Ibid.

[553] Ibid.

[554] Mishra interview.

[555] Lloyd's Register-Fairplay, Ltd. *Ports & Terminals Guide*. CDROM, Accessed: March. 28, 2006.

[556] Ibid.

[557] Ibid.

[558] (GOI) (CBEC). *Index of Customs Act, 1962.* Online Available: http://www.cbec.gov.in/cae/customs/cs-act/formatted-htmls/cs-act-idx.htm. Accessed: March 28, 2006

[559] CIA, *The World Factbook – Netherlands*. Online. Available: http://www.cia.gov/cia/publications/factbook/geos/nl.html/. Accessed: April 6, 2006.

[560] Jimena Clark, David Dollar, et al… "Maritime Transport Costs and Port Efficiency," Inter-American Development Bank Report. 2003. Online. Available: http://www.cea-uchile.cl/Iase2003/program_3.pdf. Accessed: May 1, 2006

[561] Dirk Summer, *Private Participation in Port Facilities: Recent Trends* World Bank Group: Finance, Private Sector, and Infrastructure Network. 1999. Online: Available: http://www.cancakmak.com/ppi5/book/193somme.pdf. Accessed: May 1, 2006

[562] Secretaria de Comunicacion y Transportes (SCT), "Get to Know Us," Online. Available: http://portal.sct.gob.mx:80/SctPortal/apPAMnager/Portal/Sct;jsessionid=GgGj6BBkPTmCV71MLLNTytsSKhgWpG8X3lFZQsmXf0kPRYhmt24B!-59968673!NONE?_nfpb=true&_pageLabel=sct_book_53. Accessed: June 20, 2006.

[563] Secretaria de Comunicacion y Transportes (SCT), "Principal Advancements in the Sector" SCT: Annual Report 2005, Online. Available: http://portal.sct.gob.mx:80/SctPortal/apPAMnager/Portal/Sct?_nfpb=true&_pageLabel=B28002. Accessed: June 20, 2006.

[564] Secretaria de Comunicacion y Transportes (SCT), "Structure," Online. Available: http://portal.sct.gob.mx:80/SctPortal/apPAMnager/Portal/Sct?_nfpb=true&_pageLabel=P32005. Accessed: June 20, 2006.

[565] Secretaria de Comunicacion y Transportes (SCT), "Principal Advancements in the Sector" SCT: Annual Report 2005, Online. Available: http://portal.sct.gob.mx:80/SctPortal/apPAMnager/Portal/Sct?_nfpb=true&_pageLabel=B28002. Accessed: June 20, 2006.

[566] Secretaria de Comunicación y Transportes (Secretary of Communication and Transport)

[567] Interview by Claudia Arniella with Capitan Manuel F. Gutierrez Gallardo, Assistant Director of Port Protection, APIVER, Port of Veracruz, Veracruz, Mexico. April 10, 2006.

[568] Fide y Comiso de Educación Náutica (FIDENA), "Puertos Mexicanos," Online. Available: http://www.fidena.edu.mx/. Accessed: May 5, 2006

[569] Secretaria de Economia (Secretary of Economy, SE), "Law of Exterior Commerce" Online. Available: http://www.economia.gob.mx/?P=934. Accessed: June 20, 2006.

[570] Online. Available: http://www.cddhcu.gob.mx/leyinfo/pdf/55.pdf. Accessed: June 20, 2006.

[571] Interview by Claudia Arniella with Miguel Mario Inzunza Luque, Assistant Administrator of Customs Operations, Aduana Mexico (Mexican Customs), Veracruz, Mexico, April 10, 2006.

[572] Ibid.

[573] Aduana Mexico (Mexican Customs). "Administración General de Aduanas (General Customs Administration)," Online. Available: http://www.aduanas.sat.gob.mx/aduana_mexico/A_Organigrama_AGA.htm. Accessed: June 20, 2006.

[574] Camara de Diputados (House of Representatives. "Mexican Customs Law" Online. Available: http://www.cddhcu.gob.mx/leyinfo/pdf/12.pdf. Accessed: June 20, 2006.

[575] Business Alliance for Secure Commerce (BASC) *Who We Are*, Online. Available. http://www.wbasco.org/espanol/quienessomos.htm. Accessed: May 5, 2006

[576] United States Customs and border Protection, *Customs-Trade Partnership Against Terrorism (C-TPAT): Partnership to Secure the Supply Chain.* Online. Available. http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/. Accessed: May 1, 2006

[577] U.S. Customs and Border Protection (CBP), *US/Mexico FAST Program*, Online. Available: http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/fast/us_mexico/. Accessed: May 12, 2006.

[578] Lupita Murillo "Almost a Ton of Marijuana Found Hidden in a Produce Truck," NEWS 4 KVOA Tucson, AZ. Online. Available: http://kvoa.com/Global/story.asp?S=4991879&nav=HMO6. Accessed: June 6, 2006.

[579] Sub-Committee on Customs Procedures (SCCP), *About SCCP*, Online. Available: http://www.sccp.org/about/menu.htm. Accessed: May, 5, 2006

[580] Sub-Committee on Customs Procedures (SCCP), *A Blueprint for APEC Customs Modernization, Working with Business for a Faster, Better Border.* Online. Available: http://www.sccp.org/sccplibrary/papers/blue-22.htm#Building%20the%20Future%20Framework. Accessed May 5, 2006

[581] APEC/SCCP. "About APEC/SCCP: Collective Action Plan." Online. Available: http://www.sccp.org/about/menu.htm. Accessed: June 20, 2006.

[582] "Veracruz: Leader in Automobile Shipments," APIVER. April 2006. Online. Available: http://www.apiver.com/apiwww/npop023.htm. Accessed: May 1, 2006.

[583] Joachim Bamrud, "Santos: Top Latin Port" May 30, 2006

[584] APIVER, *Companies at the Port*, Online. Available: http://148.223.221.118/apiwww/ces.htm. Accessed May 5, 2006

[585] Interview by Claudia Arniella with Vicente Angel Linares, Protection Official and Assistant Director of Operations, ICAVE, Veracruz, Mexico. April 10, 2006.

[586] Ibid.

[587] Ibid.

[588] "The Port of Veracruz Supplies over 15 Mexican States" APIVER: Important News. Noticias Importante, May 2006. Online. Available: http://www.apiver.com/apiwww/npop022.htm. Accessed: May 15, 2006

[589] Interview by Claudia Arniella with Capitan Manuel F. Gutierrez Gallardo, Assistant Director of Port Protection, APIVER, Port of Veracruz, Veracruz, Mexico. April 10, 2006.

[590] Ibid.

[591] Ibid.

[592] Interview by Claudia Arniella with Miguel Mario Inzunza Luque, Assistant Administrator of Customs Operations, Mexican Customs, Veracruz, Mexico. April 10, 2006.

[593] Secretary of Tax Administration (Servicio de Administración Tributaria or SAT) Customs Law Regulations. Online. Available. http://www.sat.gob.mx/nuevo.html. Accessed: May 1, 2006.

[594] Miguel Mario Inzunza Luque interview.

[595] Ibid.

[596] Ibid.

[597] Interview by Claudia Arniella with Miguel Mario Inzunza Luque, Assistant Administrator of Customs Operations, Mexican Customs, Veracruz, Mexico. April 10, 2006.

[598] Telephone interview with anonymous CBP official, January 2006.

[599] Alliance for the Security and Prosperity of North America, (La Alianza para la Seguridad y la Prosperidad de América del Norte or ASPAN) *About ASPAN*. Online. Available. http://www.aspan.presidencia.gob.mx/?c=31. Accessed: May 12, 2006

[600] Walters, Todd M., "The Mexico-U.S. Parthernship Enhancing Our Common Security," *The Institue for Foreign Policy Analysis, Inc,* (2005), pp. 5-6. Online.

Available: http://www.ifpa.org/pdf/Mex_US_Wrkshp_Report.pdf. Accessed: May 1, 2006.

[601] Interview by Claudia Arniella with Capitan Manuel F. Gutierrez Gallardo, Assistant Director of Port Protection, APIVER, Port of Veracruz, Veracruz, Mexico. April 10, 2006.

[602] Vicente Angel Linares, Protection Official and Assistant Director of Operations, ICAVE, Veracruz, Mexico

[603] Phone interview by Claudia Arniella with Capitan Raymundo Mata Contreras, Deputy Director General, Secretary of Communication and Transport, Mexico City, Mexico, April 10, 2006.

[604] Telephone interview with anonymous CBP official, January 2006.

[605] CIA, *The World Factbook – Netherlands*. Online. Available: http://www.cia.gov/cia/publications/factbook/geos/nl.html/. Accessed: January 3, 2006.

[606] Ministerie van Verkeer en Waterstaat (MVW). Online. Available: http://www.verkeerenwaterstaat.nl/. Accessed: February 18, 2006.

[607] MVW. Online. Available: http://www.rijkswaterstaat.nl/rws/projects/wocb/cissitened/netherlands/main.htm. Accessed: June 19, 2006.

[608] CASR: Canadian Defense Policy, Foreign Policy & Canada-US Relations. *Port Security, Coastal Patrol & Maritime Defence* Online. Available: http://www.sfu.ca/casr/id-sen-holland.htm. Accessed: June 18, 2006.

[609] Ibid.

[610]Ibid.

[611] CASR. Online. Available: http://www.sfu.ca/casr/id-sen-holland.htm. Accessed: June 19, 2006.

[612] Dutch Immigration. *The Rotterdam-Rijnmond Seaport Police*. Online. Available: http://www.dutch-immigration.nl/uk_info_rivpol.htm. Accessed: June 13, 2006.

[613] Ibid.

[614] Ibid.

[615] Ibid.

[616] Ibid.

[617] Ibid.

[618] Email from Jan Kamp, Project Manager, Customs Rotterdam, "Betr: Questions for US Congress/ University of Texas Research Project," to Matt Williams, April 10, 2006.

[619] *Ministry of Finance*. Netherlands. Online. Available: http://www.minfin.nl/default.asp?CMS. Accessed: March 26, 2006.

[620] *Tax and Customs Administration. Dutch Ministry of Finance*. Online. Available: http://www.belastingdienst.nl/organisatie/en/organisatie-12.html/. Accessed: March 26, 2006.

[621] Ibid.

[622] Ibid.

[623] Seaports: Anchors of the Economy – National Seaports Policy 2005-2010. Dutch Ministry of Transport, Public Works, and Water Management. The Hague. October, 2004.

[624] European Union. *European Commission Homepage.* Online. Available: http://ec.europa.eu/justice_home/fsj/customs/fsj_customs_intro_en.htm. Accessed: June 20, 2006.

[625] Ibid.

[626] Gibson, Sean (Ed.). Ports & Terminals Guide 2005-2006. Volume 3. Lloyd's Register-Fairplay, Ltd.. p. 3,209-211.

[627] Interview by Amy Shuart and Matt Williams with Sander Doves, Policy Advisor, Strategy Port Infrastructure and Maritime Affairs, Rotterdam, Netherlands, January 9, 2006.

[628] Gibson, Sean (Ed.). Ports & Terminals Guide 2005-2006. Volume 3. Lloyd's Register-Fairplay, Ltd. p. 3,209-211.

[629] Email from Sander Doves, Policy Advisor, Strategy Port Infrastructure and Maritime Affairs, "Re: Questions" to Amy Shuart, May 6, 2006.

Sander email

[630] *Profile of the Non-Executive Board, Port of Rotterdam Authority*. Online. Available: http://www.portofrotterdam.com/mmfiles/Profile%20Non-Executive%20Board_tcm26-9424.pdf. Accessed: June 15, 2006.

[631] *Port of Rotterdam, Port of Rotterdam Authority*. Online. Available: http://www.portofrotterdam.com/en/port_authority/index.jsp/. Accessed: April 2, 2006.

[632] Ibid.

[633] *Profile of the Non-Executive Board, Port of Rotterdam Authority*. Online. Available: http://www.portofrotterdam.com/mmfiles/Profile%20Non-Executive%20Board_tcm26-9424.pdf. Accessed: June 15, 2006.

[634] Ibid.

[635] Sander email.

[636] Sander email.

[637] Sander email.

[638] Ibid.

[639] Sander email.

[640] Sander email.

[641] Sander email.

[642] Sander email.

[643] Sander email.

[644] Sander email.

[645] Sander email.

[646] Doves interview.

[647] Ibid.

[648] Ibid.

[649] Ibid.

[650] Doves interview.

[651] Ibid.

[652] *Aon Netherlands, Port Facility Security Toolkit*. Online. Available: www.portsecuritytoolkit.com/. Accessed: January 18, 2006.

[653] Ibid.

[654] *Tax and Customs Administration. Dutch Ministry of Finance*. Online. Available: http://www.belastingdienst.nl/organisatie/en/organisatie-10.html/. Accessed: March 26, 2006.

[655] Gibson, Sean (Ed.). Ports & Terminals Guide 2005-2006. Volume 3. Lloyd's Register-Fairplay, Ltd. p. 3,210-211.

[656] *Port of Rotterdam*. Online. Available: http://www.portofrotterdam.com/en/business/Customs/index.jsp/. Accessed: March 26, 2006.

[657] Interview by Amy Shuart and Matt Williams with Jan Kamp, Project Manager, Customs Rotterdam, Rotterdam, Netherlands, January 9, 2006.

[658] http://www.energy.gov/news/1115.htm (online).

[659] GAO Report 05-375, pg. 2

[660] GAO Report 05-375, pg. 4

[661] Ibid, pg. 15

[662] Ibid, pg. 12

[663] *U.S. Consulate, Hong Kong*. U.S. Department of State. Online. Available: http://www.usconsulate.org.hk/ushk/others/2002/080801.htm/. Accessed: March 26, 2006.

[664] *U.S. Department of Homeland Security, Customs and Border Patrol.* Online. Available: http://www.cbp.gov/xp/cgov/newsroom/press_releases/archives/legacy/2002/82002/08262002.xml/. Accessed: March 26, 2006.

[665] Kamp interview.

[666] Ibid.

[667] Ibid.

[668] CIA, *The World Factbook, South Africa*. Online. Available: http://www.cia.gov/cia/publications/factbook/geos/sf.html. Accessed: March 24, 2006

[669] National Port Authority (NPA), *The South African Ports Yearbook 2004*. (United Kingdom, 2003) p. 6

[670] Transnet, *Transnet – South Africa's Largest Transport and Logistics Company*. Online. Available: http://www.transnet.co.za/BrowserDefault.aspx?tabid=672. Accessed: March 25, 2006

[671] NPA, *The South African Ports Yearbook 2004*, p. 6

[672] South African Port Operations, *South African Port Operations*. Online. Available: http://www.saponet.co.za/about.asp. Accessed March 25, 2006

[673] Interview by Troy Roberts with Pretoria Port Security Stakeholders, Mrs. Myra van der Merwe, Mr. Gerrie Mulder, Mr. Saleem Modak, Ms. Gugu Ndebele, Mr. Kerwin Rampono, Mr. Andrew Maswanganye, Mr. Billy Mokale, and Mr. Lucas Haluodi, Pretoria, South Africa, January 12, 2006.

[674] South African Police Services, *South African Police Services, Department for Safety and Security*, Online. Available: http://www.saps.gov.za/default.htm. Accessed: March 25, 2006

[675] Pretoria Stakeholders interview.

[676] NPA, *National Ports Authority*, South *Africa*. Online. Available: http://www.npa.co.za/. Accessed: March 28, 2006.

[677] NPA, *The South African Ports Yearbook 2004*. p. 6.

[678] Ibid.

[679] Cheryl van der Merwe, "Securing SA's Ports," *CEO Magazine, National Port Authority,* Vol.5*, No*. 3 – 2006, p. 43.

[680] Ibid., p.44.

[681] Ibid., p 45.

[682] Republic of South Africa, Government Gazette Staatskoerant, *Merchant Shipping (Maritime Security) Regulations 2004,* Vol. 468, No.26488, (Pretoria, South Africa, June 21, 2004).

[683] *South African Revenue Service Act, 1997*, 5 September 1997.

[684] Ibid.

[685] Ibid

[686] Ibid.

[687] South African Revenue Service, *South African Revenue Service*. Online. Available: http://www.sars.gov.za/. Accessed: March 28, 2006.

[688] Daily News. *SARS in billion-rand anti-smuggling campaign.* Online. Available: http://www.int.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20060127093522365C950958. Accessed: January 27, 2006. This information was confirmed at the Durban Port Security Stakeholder meeting on January 10, 2006 with SARS representative Romeo Minnie.

[689] Lloyd's Register-Fairplay, Ltd. "Ports and Terminals Guide, 2006," CD-ROM. Accessed: 25 March 2006.

[690] Interview by Troy Roberts with Cape Town Stakeholders, Mr. Paul Booysen, Capt. Rufus Lekala, and Mrs. Selma Schwartz, Cape Town, South Africa, January 9, 2006.

[691] Ibid.

[692] Ibid.

[693] Ibid.

[694] NPA, *The South African Ports Yearbook 2004*, p. 133.

[695] Ibid.

[696] Van der Merwe, "Securing SA's Ports," p. 43-44.

[697] Cape Town interview.

[698] Interview by Troy Roberts withDurban Stakeholders, Mr. Hennie Strydom, Mr. Justice Blose, Mr. Romeo Minnie, Mr. Qiniso Mzobe, Mr. Vusumzi Tito, and Mr. Castro Khwela, Durban, South Africa, January 10, 2006.

[699] Durban and Cape Town interviews.

[700] Ibid.

[701] CIA, *The World Factbook, South Africa* (online).

[702] BBC NEWS, *South Africa Security Staff on Strike*. Online. Available: http://news.bbc.co.uk/2/hi/africa/4837708.stm. Accessed: April 1 2006.

[703] Durban interview.

[704] Durban and Cape Town interviews.

[705] Pretoria interview.

[706] Van der Merwe, "Securing SA's Ports," p. 45-46.

[707] Pretoria interview.

[708] Durban and Cape Town port-security stakeholders interviews.

[709] Van der Merwe, "Securing SA's Ports," p. 45-46.

[710] Ibid.

[711] Interview by Katy Koch with Mike Toddington, Houston, Texas, February 3, 2006.

[712] Pretoria interview.

[713] Van der Merwe, "Securing SA's Ports," pp. 44-45.

[714] Pretoria, Durban and Cape Town interviews.

[715] Pretoria interview.

[716] Pretoria, Durban and Cape Town interviews.

[717] Pretoria interview.

[718] Durban and Cape Town interviews.

[719] Cape Town interview.

[720] South African Revenue Service (SARS), *South African Revenue Service.* Online. Available: http://www.sars.gov.za/. Accessed: April 1, 2006.

[721] Durban interview.

[722] U.S. Customs and Border Protection, *Government of South Africa Becomes First African Nation to Implement their Container Security Initiative, Begins Targeting and Pre-screening Cargo Destined for U.S.* Online. Available:

www.cbp.gov/xp/cgov/newsroom/press_releases/archives/cbp_press_releases/0122003/12022003.xm1. Accessed: March 30, 2006.

[723] Durban interview.

[724] Ibid.

[725] Pretoria, Durban and Cape Town interviews.

[726] (GOI), The Central Industrial Security Force Act(CISF Act), No.50 of 1968. March 10 ,1969. (As modified vide Act No.14 of 1983, 20 of 1989 and 40 of 1999). Online. Available: http://cisf.nic.in/eng_ver.htm. Accessed: February 2, 2006.